Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

UNITED STATES OF AMERICA, ET AL., Plaintiffs, v. GOOGLE LLC, Defendant.	Civil Action No.: 1:23-cv-00108 (LMB/JFA)

Expert Report of Anthony J. Ferrante

January 23, 2024

Introduction

1. I, Anthony J. Ferrante, am a Senior Managing Director and Global Head of Cybersecurity at FTI Consulting, Inc. ("FTI"). I have been retained by counsel ("Counsel") for Google LLC .

2. In this report, I opine on certain issues based on cybersecurity, privacy and security relating to digital advertising.

3. Except as otherwise noted, I have personal knowledge as to all the information set forth in this report. All facts and opinions included in this report are based upon my personal experiences and knowledge relating to cybersecurity, information supplied to me by Counsel, and my review of other relevant information related to the Plaintiffs' claims.

Summary of Opinions

8. With the explosion of digital advertising and online activity, the threat of malicious cyber activity has only exponentially followed. From my law enforcement, national security, and industry experience, as well as my review of documents produced in connection with this case, and supplemental open source materials set forth in Appendix B: Materials Relied On, it is my opinion that:

    - Malvertising and digital advertising fraud are now a persistent and pernicious form of organized crime, presenting a substantial threat to global Internet users and all participants in the digital advertising ecosystem and costing participants in the ecosystem billions of dollars every year. The global costs related to digital advertising fraud as a whole have grown exponentially over the past five years (2018-2023), from approximately $35 billion to $100 billion USD;[1]

    - Google stood out as an early industry leader in the face of this rising threat. Google developed and collaborated with partners to set and invest in standards and protocols for industry-wide use to improve the entire advertisement ecosystem and make it safer for all participants, including through its role in developing ads.txt and collaborating with industry working groups such as the Interactive Advertising Bureau Technology Lab and Trustworthy Accountability Group;

    - The open environment that the header bidding auction method provides, and its lack of integration between exchanges and its participants, creates opportunities for malicious actors to take advantage of Internet users and advertisers; and

    - Google's development of the Open Bidding methodology and its integrated environment enabled Google to bolster security through the application of its tools and standards at all ends of the process.

I have not evaluated other aspects of this case, nor have I been asked to opine on the case in a wider scope.

[1] *Estimated cost of digital advertising fraud worldwide in 2018 and 2023*, Statista Research Department (Jan. 10, 2023), https://web.archive.org/web/20230911041343/https://www.statista.com/statistics/677466/digital-ad-fraud-cost/.

Introduction: Advertising Fraud and Malvertising

9. Advertising (ad) fraud and malvertising are monumental threats facing digital advertisers and businesses. Ad fraud targets ad traffic while malvertising targets ad quality. Ad fraud aims to steal ad revenue from publishers via invalid traffic, whereas malvertising is an attempt to steal ad revenue, publisher data, and user data.[2]

10. Ad fraud is an attempt to deceive advertising platforms into thinking that fake activity on the network is real user behavior for the purpose of financial gain. Ad fraud occurs when non-humans, or invalid traffic ("IVT") such as click bots,[3] interact with ads so that the publisher makes money at the expense of the advertiser, since the ads are not seen, or clicked on, by a real user. Ad fraud significantly impacts advertisers as it diminishes their Return on Ad Spend ("ROAS").

11. Malicious advertising, or "malvertising," describes nefarious content in an advertisement itself. Malicious ads target users, their data, or their device with fraudulent content designed to trick ad viewers into interacting with the malicious ad as if it were legitimate. Once clicked, the malicious advertisement may install malware on the user's device or redirect the user to a malicious website that solicits sensitive information. This is referred to as a "malvertising attack."

12. Once malware[4] is delivered and installed through a malvertising attack, it can damage files, redirect Internet traffic, monitor the user's activity, steal data, or set up backdoor access points to the user's device. Malware may also delete, block, modify, leak or copy data, which can then be sold on the dark web, sold back to the user for ransom, or otherwise used in furtherance of a malicious actor's unlawful purposes.[5]

13. Malicious ads are difficult to identify due to their various forms (outlined below) and ability to be placed through ad servers on legitimate, reputable, and trustworthy websites. As a result, billions of website users are at daily risk of falling victim to a malicious ad and remain largely unaware of the threat lurking on even the most popular and trusted websites and platforms. And despite improvements in the digital ad landscape, the Trustworthy Accountability Group ("TAG") estimates that today nearly 1 in every 100 ad impressions and more than 20% of user sessions could be impacted by malvertising.[6]

---

[2] Neeraja Shanker, *Advertising fraud, malvertising, and its impact on publishers*, Blockthrough (Sept. 1, 2022), https://blockthrough.com/blog/advertising-fraud-and-malvertising/.

[3] Bot, short for robot, is a software program or script that performs automated, repetitive, predefined tasks that aim to imitate or replace human activity.

[4] Malware is most often defined as a malicious program or code that is harmful to systems.

[5] Bart Lenaerts-Bergmans, *What is Malvertising*, CrowdStrike (Oct. 17, 2022), https://www.crowdstrike.com/cybersecurity-101/malware/malvertising/.

[6] *Share Threat Intelligence*, The Trustworthy Accountability Group (last accessed Jan. 19, 2024), https://www.tagtoday.net/threat-sharing.

The Threat Actors

14. Threat actors are malicious groups or individuals who intentionally exploit weaknesses in an information system, or gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks. They take advantage of technical vulnerabilities, use social engineering against online users,[7] and promote false or misleading content online to influence individuals' behavior and beliefs.[8]

15. The threat actors engaging in ad fraud vary based on intentions, but are mainly cybercriminals, Blackhat marketers, and even ad networks themselves. Criminals most often commit ad fraud to generate revenue, but also to damage competitors' reputations or deplete rivals' advertising budgets.[9] In either case, money is stolen from legitimate advertisers often to fuel international criminal enterprises.

16. Organized crime members gravitate towards ad fraud because of the risk to reward ratio. It has the potential for a large payout with relatively low risk and effort. Ad fraud is expected to become the largest market for organized crime by 2025, and likely to exceed $50 billion globally, second only to the drugs trade as a source of income for organized crime.[10] Malvertising is also rooted in organized crime and its ecosystem and is believed to be connected to the funding of organized crime rings, often in Eastern Europe, including the Russian Business Network. The self-proclaimed "King of Fraud" Aleksandr Zhukov, a Russian national, was sentenced to ten years in prison for the digital advertising fraud scheme known as "Methbot," which took over $7 million from U.S. advertisers, publishers, platforms, and others in the U.S. digital advertising industry between September 2014 and December 2016.[11] Methbot was the largest and most profitable botnet operation until "3ve" (outlined in more detail below): Zhukov's sophisticated bot army watched 300 million video ads per day on over 6,000 spoofed websites made to look like premium publisher websites.[12]

17. During my time at the FBI, we saw maltervising as a vector that was being exploited in increasing volume. In one case I worked on in 2011, charges were brought against six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that

---

[7] Social engineering uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

[8] Department of Health and Human Services Office of Information Security, *Types of Cyber Threat Actors That Threaten Healthcare* (Jun. 8, 2023), https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf.

[9] *Who Is Behind Programmatic Advertising Fraud?*, Anura (last visited Jan. 12, 2024), https://www.anura.io/fraud-tidbits/who-is-behind-programmatic-advertising-fraud.

[10] *WFA issues first advice for combatting ad fraud*, World Federation of Advertisers (Jun. 6, 2016), https://wfanet.org/knowledge/item/2016/06/06/WFA-issues-first-advice-for-combatting-ad-fraud.

[11] Press Release, *Russian Cybercriminal Sentenced to 10 Years in Prison for Digital Advertising Fraud Scheme*, United States Attorney's Office for the Eastern District of New York (Nov. 10, 2021), https://www.justice.gov/usao-edny/pr/russian-cybercriminal-sentenced-10-years-prison-digital-advertising-fraud-scheme.

[12] *Methbot: Then and Now,* Human Blog (Jun. 1, 2021), https://www.humansecurity.com/learn/blog/methbot-then-and-now.

infected over four million computers with malware in over 100 countries. Of the computers infected, at least 500,000 were in the United States, including computers belonging to U.S. government agencies, such as NASA; educational institutions; non-profit organizations; commercial businesses; and individuals. The malware altered the settings on infected computers enabling the threat actors to digitally hijack Internet searches and reroute computers to certain websites and advertisements, with the threat actors pocketing at least $14 million in fraudulent advertising fees.[13]

18. That same year, the FBI's Minneapolis office launched an investigation into an international criminal group using malvertising to spread its scareware product. Scareware is malicious software that poses as legitimate computer security software and claims to detect a variety of threats on the affected computer that do not actually exist. Users are informed they must purchase the scareware product, or anti-virus software, in order to repair their computer and are hit with aggressive and repetitive notifications until they supply their credit card number. Two individuals in Latvia were charged with creating a fake advertising agency and claiming to represent a hotel chain that wanted to purchase online advertising space on a Minneapolis newspaper's website. After the ad was verified by the paper and posted, the threat actors changed the ad's computer code so that visitors to the site became infected with a malicious software program that launched scareware on their computers. That scheme cost its victims about $2 million.[14] The threat actors have only become more sophisticated over time and can carry out ad fraud and malvertising in multiple forms, outlined further below.

The Impact of Ad Fraud and Malvertising on Advertisers, Publishers and Consumers

19. Ad fraud and malvertising have a substantial and detrimental impact on all parties involved in the digital advertising ecosystem, including: website visitors, website hosts, the legitimate organizations advertising their products, as well as the advertisement publishers themselves. The prevalence of both ad fraud and malvertising is continuously increasing, and becoming more sophisticated as the digital landscape evolves.

20. The most immediate harm malvertising causes is towards website users, resulting in sensitive information being compromised.

---

[13] Press Release, *Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Million of Computers Worldwide and Manipulated Internet Advertising Business*, The Federal Bureau of Investigation (Nov. 9, 2011), https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business.

[14] Press Release, *Latvian Cybercriminal Extradited For "Scareware" Hacking Scheme That Caused Millions of Dollars in Loss*, United States Department of Justice Office of Public Affairs (Jun. 12, 2017), https://www.justice.gov/opa/pr/latvian-cybercriminal-extradited-scareware-hacking-scheme-caused-millions-dollars-loss.

21. Advertisers may also have their potential ad reach limited by malvertising, as it causes users to be more suspicious of digital ads going forward, especially if exposed to deceptive ads masquerading as a legitimate product or organization. Not only can malvertising have a negative impact on websites where users have personally experienced malvertising, it can lead to users installing advertisement-blocking tools.

22. Advertisers are adversely impacted by ad fraud because digital ad fraud accounts for approximately $1 for every $3 spent on digital ads.[15] The World Federation of Advertisers, which represents 100 of the world's biggest brand owners and 60 national advertiser associations, estimated in 2016 that 10% to 30% of advertising is fraudulent and not seen by consumers.[16] Other analysts estimate that 8% of display advertising impressions are fraudulent and 14% of video ads are fraudulent.[17] In 2022, ad fraud surpassed credit card fraud in terms of both money lost and as a percentage of the industry revenue.[18]

23. Publishers make money by running ads, with digital publishers generating revenue by offering their readers as audiences for advertisers. If their website does not show the ads of the advertiser who paid for the ad inventory, then publishers lose anticipated revenue from running ads. For publishers, malvertising and ad fraud tactics also can cause significant damage to a site's brand reputation, as well as contribute to ad revenue and traffic loss. When an auto-redirect ad (seemingly legitimate ads that redirect a user to a malicious website and can garner sensitive user information) appears on a publisher's website, that ad negatively affects the user's trust and confidence in the publisher and they are less likely to revisit that site.

24. The global costs related to digital advertising fraud as a whole have grown exponentially over the past five years (2018-2023), from $35 billion to $100 billion USD, as displayed in Figure A. In 2022 alone, digital ad fraud costs worldwide were believed to reach $81 billion,[19] and 22% of the total value of global spend of digital advertising in 2023 is expected to be lost to ad fraud.[20] Juniper Research forecasts that the global potential advertising spend lost to fraud will rise to $172 billion (23% of the total digital ad spend) by 2028, and 42% of the ad spend lost to ad fraud will be in North America.[21]

---

[15] George Slefo, *Report: For Every $3 Spent on Digital Ads, Fraud Takes $1*, AdAge (Oct. 22, 2015), https://adage.com/article/digital/ad-fraud-eating-digital-advertising-revenue/301017.

[16] Robert Cookson, *Digital advertising: Brands versus bots*, The Financial Times (Jul. 18, 2016), https://www.ft.com/content/fb66c818-49a4-11e6-b387-64ab0a67014c.

[17] *The Economic Cost of Bad Actors on the Internet* at Page 12, University of Baltimore (2020), https://info.cheq.ai/hubfs/Research/Economic-Cost-BAD-ACTORS-ON-THE-Internet-Ad-Fraud-2020.pdf.

[18] *The Economic Cost of Bad Actors on the Internet* at Page 5, University of Baltimore (2020), https://info.cheq.ai/hubfs/Research/Economic-Cost-BAD-ACTORS-ON-THE-Internet-Ad-Fraud-2020.pdf.

[19] *Estimated cost of digital advertising fraud worldwide in 2018 and 2023*, Statista Research Department (Jan. 10, 2023), https://web.archive.org/web/20230911041343/https://www.statista.com/statistics/677466/digital-ad-fraud-cost/.

[20] *Quantifying the Cost of Ad Fraud: 2023-2028* at Slide 2, Juniper Research (last accessed Jan. 12, 2024), https://fraudblocker.com/ad-fraud-data-facts?utm_campaign=pr.

[21] *Quantifying the Cost of Ad Fraud: 2023-2028* at Slide 2, Juniper Research (last accessed Jan. 12, 2024), https://fraudblocker.com/ad-fraud-data-facts?utm_campaign=pr.

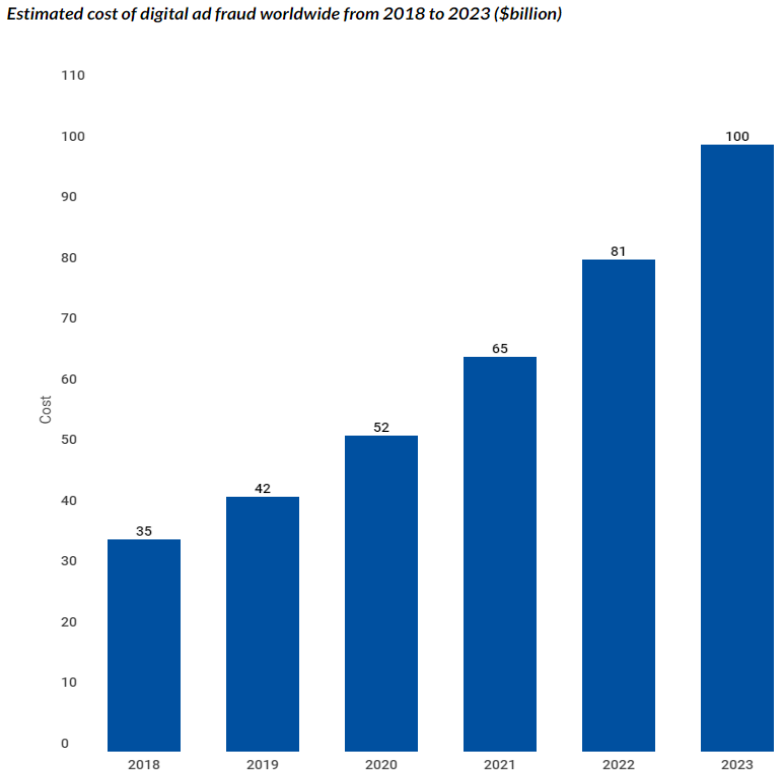


Figure A: Estimated cost of digital ad fraud worldwide from 2018-2023 in billions (Statista)[22]

Forms of Advertising Fraud and Malvertising

25. Malvertising and advertising fraud may prove difficult to detect and identify due to the various forms and tactics a threat actor may employ in an attempt to compromise an individual or business.

Auto-Redirect Ads

26. Auto-redirect ads are a form of ad fraud that will redirect a user to an ad's landing page, even if the user did not interact with it. While they appear to be legitimate advertisements, they redirect a user to a website controlled by a threat actor. Auto-redirect ads are one of the most difficult forms of malvertising to detect and accounted for 48% of all malvertising in 2020.[23] The malicious website may contain malware that is then downloaded to the user's device, or could be used to spoof a legitimate product or solicitation in order to garner sensitive information from the user. For publishers, auto-redirect ads steal traffic from their website and revenue that

[22] *Estimated cost of digital advertising fraud worldwide in 2018 and 2023*, Statista Research Department (Jan. 10, 2023), https://web.archive.org/web/20230911041343/https://www.statista.com/statistics/677466/digital-ad-fraud-cost/.
[23] *How to Stop Forced Auto Redirect Advertising*, GeoEdge (last accessed Jan. 12, 2024), https://www.geoedge.com/auto-redirects/.

could have been earned from a legitimate ad.[24] In order to combat auto-direct ads, a user may install an adblocker, which, in turn, affects the publisher's earnings.

27. Figure B below is a common example of an auto-redirect ad. A user opens a webpage and a pop-up appears with an opportunity to claim a prize. If the user clicks to claim the prize, or tries to close the pop-up, the user is redirected to another webpage that deploys malicious code.

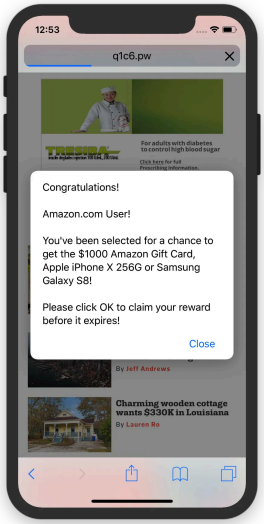


Figure B - Example of a redirect ad[25]

Ad Injectors

28. Ad Injectors are programs that take over a user's browser session to insert new ads, or replace the existing ads, into the pages a user will visit while browsing the web.[26] As seen in Figure C, none of the ads displayed on Amazon are organic to the page; the page is entirely infected with ad injectors. These injected advertisements can even show on sites that are supposed to be ad-free (e.g. Apple). In Figure C, the H&R Block ad on Apple is another example of an injected ad. These ads originate from an extension installed on the user's browser that contains software that injects unwanted ads into a user's browser. The software is then dispersed by a network of affiliates who are paid a commission when a user clicks on an injected ad. This creates security and data privacy concerns for the infected user, and lost revenue for advertisers who paid to display an ad that will be replaced by an injected ad.

[24] *How to Stop Forced Auto Redirect Advertising*, GeoEdge (last accessed Jan. 12, 2024), https://www.geoedge.com/auto-redirects/.

[25] Winston Hearn, *Why ads keep redirecting you to scammy sites and what we're doing about it*, Vox Media (Jan. 22, 2018), https://product.voxmedia.com/2018/1/22/16902862/why-ads-redirect-to-giftcards-and-what-were-doing-to-secure-them.

[26] Kurt Thomas et al., *Ad Injection at Scale: Assessing Deceptive Advertisement Modifications* at 2, IEEE Symposium on Security and Privacy (2015), https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43346.pdf.

29. Some of the biggest advertising giants and publishers in the world fall victim to injected ads and the primary actors behind injected ads go by the name “215 Apps” or “Engaging Apps.” These actors have built a network of browser extensions that give consumers the impression they will be able to have an added benefit, like downloading videos, but instead inject ads on those sites.

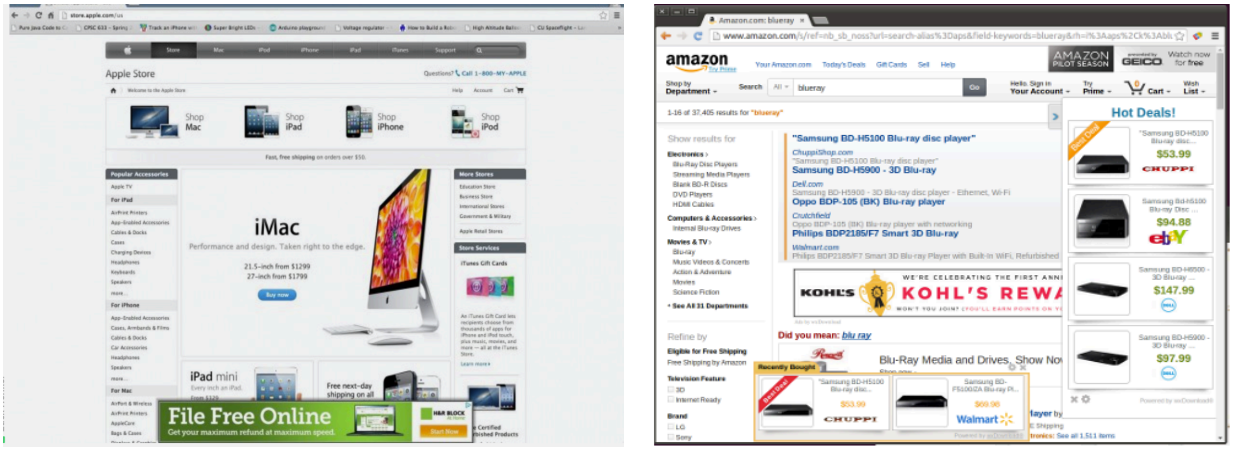


Figure C: Sample of ad injection on different shopping properties. None of the ads displayed are organic to the page.[27]

Bots & Botnets

30. A computer bot (short for “robot”) is a software application programmed to execute specific predefined and repetitive tasks or mimic human activity and behavior. Bots may be used in a harmless manner, such as an individual using a bot to automate or script a simple task. On the other hand, a botnet may be used to visit a website and maliciously interact with the advertisements on the webpage. As a publisher receives payment for every click generated by an advertisement on a website, a fraudulent actor may use a botnet to repeatedly “spam” click advertisements on their websites. The use of botnets can lead to false and skewed data due to impressions, page views, and clicks that are generated from bots but believed to be generated from legitimate Internet users. While they can carry out useful, often mundane, tasks at a faster speed than a human, they also come in the form of malware. Malicious bots can be used in the background, unknowingly to the user, to generate invalid traffic to websites or advertisements.

31. Botnet (short for "robot network”) refers to an assembly of computers that malware has compromised, which are remotely controlled by an attacker, or a “bot herder.” Bot-herders have the ability to direct botnets - which can include millions of bots - to specific networks, systems, or websites. In ad fraud, the owner of the botnet can direct the bots to a website on which fraudulent ads have been placed by the fraudulent actor in order to generate fake revenue or launch massive, highly damaging denial-of-service (DDoS) attacks on targeted systems or networks.

[27] Kurt Thomas et al., *Ad Injection at Scale: Assessing Deceptive Advertisement Modifications* at 2, IEEE Symposium on Security and Privacy (2015), https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43346.pdf; Nate Anderson, *How a banner ad for H&R Block appeared on apple.com—without Apple’s OK*, ARS TEchnica (Apr. 7, 2013), https://arstechnica.com/tech-policy/2013/04/how-a-banner-ad-for-hs-ok/.

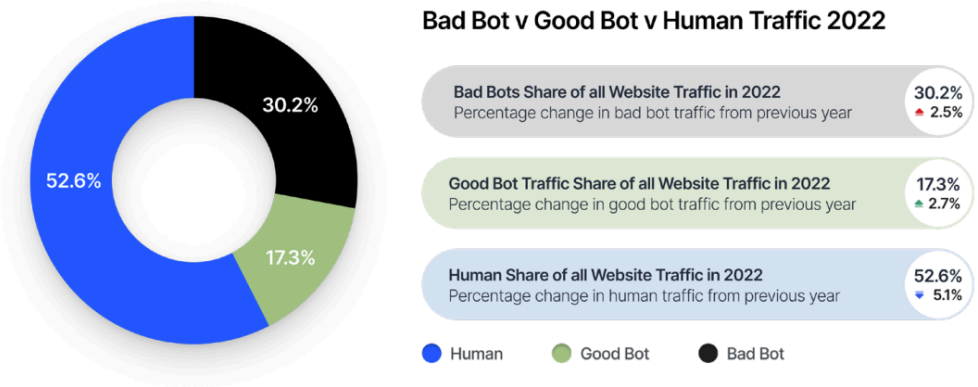


Figure D - Bot and human traffic online[28]

32. According to a study by Imperva (Figure D), a cyber security software and services company, nearly half (47.4%) of the Internet traffic in 2022 consisted of bots, compared to 42.3% in 2021.[29] Of that automated traffic, 30.2% were bad (malicious) bots, a 2.5% increase from 27.7% in 2021. The percentage of human traffic continues its downward trend, from 57.7% in 2021 to 52.6% in 2022.

Drive-By Download Attack

33. A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of cyber threats. In some instances, threat actors may utilize what is known as a drive-by download attack, a malvertising strategy where the threat actor, having obtained the trust of the advertisement exchange, is able to place a malicious advertisement containing an exploit kit within a legitimate website.[30] An exploit kit is a piece of malware designed to automatically identify and exploit a wide array of vulnerabilities within a user's hardware when the website is visited by a user. The exploit kit can be run through authorized or unauthorized execution.

34. Authorized execution is any type of drive-by download that requires user input to execute, whether it be clicking a fake download link, a fake button prompt, or any similar façade. Unauthorized downloads have the same end goal as authorized downloads, but deliver their malware without user interaction. The malware is triggered by simply visiting the target website. These exploit kits can be more dangerous than targeted, software-specific exploits as they can be deployed to an extremely broad range of users. Once an exploit kit has been installed onto a user's device and identifies exploitable vulnerabilities on the device, it can create a remote

[28] *2023 Bad Bot Report* at Page 5, Imperva (last accessed Jan. 12, 2024), https://www.imperva.com/resources/reports/2023-Imperva-Bad-Bot-Report.pdf.
[29] *2023 Bad Bot Report* at Page 5, Imperva (last accessed Jan. 12, 2024), https://www.imperva.com/resources/reports/2023-Imperva-Bad-Bot-Report.pdf.
[30] *TAG Malvertising Taxonomy* at Page 10, The Trustworthy Accountability Group (Nov. 2022), https://2848641.fs1.hubspotusercontent-na1.net/hubfs/2848641/TAG%20Malvertising%20Taxonomy_Nov2022.pdf?__hstc=74746893.272ca4fb7e5fe45693f4f2ef30e609bb.1705033167002.1705033167002.1705033167002.1&__hssc=74746893.1.1705033167002&__hsfp=1135167407&hsCtaTracking=f8fc1c89-ae09-4055-bf13-7206459219b8%7C1651298a-55e8-4a3f-b504-171ac937ccf5.

channel for the threat actor to install malware or perform a variety of actions. This exploit kit may ultimately allow for the threat actor to exfiltrate sensitive or financial information directly from the device, hold and encrypt the user's information for a ransom, or utilize the system as part of a botnet. Regardless of the actions taken by the threat actor and exploit kit, users may often remain unknowing throughout the entire process until their information has been compromised.

Domain Spoofing

35. Domain spoofing is the practice of bad actors disguising themselves as premium publishers in the ad-buying process by closely impersonating the domain of a legitimate and reputable organization. The buyers believe that their ads are being delivered on trustworthy and premium sites (e.g. *The New York Times*), but in reality the ads are placed on an unknown site with lower-quality (or bot) traffic with advertising dollars going directly to bad actors. Users may believe they have reached the legitimate website they seek but end up on a fraudulent domain. In 2017, an investigation by *The Financial Times* showed that $1.3 million worth of fake "FT.com" ad space was being sold each month.[31]

Cookie Stuffing

36. A cookie is a small piece of text data that websites store on a user's computer or device when they access a website. Cookie stuffing is a deceptive practice where a third-party drops multiple affiliate/tracking cookies into a user's browser without their knowledge or consent. This technique allows the affiliates to claim commissions for sales or conversions they did not genuinely contribute to, essentially "stealing" the credit and commission from other legitimate affiliates or merchants. A prominent example is when eBay, in 2017, reported that they fell victim to a $35 million cookie stuffing scheme in which two marketers rigged eBay's system to fraudulently credit them with sales they did not generate. The marketers accomplished this fraud by planting unknowing users with hundreds of thousands of cookies. The cookies signaled that the marketers should get a cut of every sale on eBay involving a user with one of these fake cookies, even though the cookies did nothing to promote eBay.[32]

Pixel Stuffing

37. Pixel stuffing occurs when an actor embeds a standard ad with a fraudulent pixel that is "stuffed" with multiple ads. These 1x1 pixels are so small that they are invisible to the naked eye. Users,

[31] Jack Marshall, *Financial Times Finds Counterfeit Ad Space Was Offered by at Least Six Companies*, The Wall Street Journal (Oct. 9, 2017), https://www.wsj.com/articles/financial-times-finds-counterfeit-ad-space-was-offered-by-at-least-six-companies-1507563713.

[32] Jim Edwards, *Web Marketer Facing Prison Claims eBay Turned A Blind Eye To A $35 Million Alleged Fraud*, Business Insider (Aug. 30, 2014), https://www.businessinsider.in/tech/web-marketer-facing-prison-claims-ebay-turned-a-blind-eye-to-a-35-million-alleged-fraud/articleshow/41232580.cms.

although unaware, are technically viewing multiple ads once the page loads and the actors therefore receive compensation for the fraudulent impressions from the stuffed ad.[33]

Ad Stacking

38. Ad stacking is a type of ad fraud in which multiple ads are placed or "stacked" on top of each other in a single ad placement. Although only the top ad is visible to the user, a single click or impression is registered for every ad in the stack, enabling the actor to bill multiple advertisers, and leading some advertisers to pay for fake clicks and/or impressions.

[33] *Digital Ad Fraud Handbook* at Page 10, IAB Australia (last accessed Jan. 12, 2024), https://m.iabaustralia.com.au/asset/445:digital-ad-fraud-handbook.pdf.

Detailed Opinions

Google's Steps to Address Malvertising and Advertising Fraud in the Digital Advertising Ecosystem

39. Malvertising first surfaced in 2007 and skyrocketed in 2014 with a 325% attack increase reported by security firm Cyphort.[34] Advertising fraud similarly reached a concerning level in 2014 when 36% of advertising traffic was generated by machines, causing advertisers to think they were paying for human views when they were not.[35]

40. By design, ad fraud and malvertising are difficult for consumers, publishers and advertisers to detect and prevent. But Google has leveraged its technology, resources, and talent to successfully contain ad fraud and malvertising campaigns. In 2014, Google acquired Spider.io's anti-fraud team led by the company's founder and botnet-fighting specialist Douglas de Jager.[36] The Spider.io staff and Google's team combined to dramatically speed up the fight against ad fraud. Google uses a combination of automated and manual reviews to analyze websites and advertisements for potential fraud and malware.[37] Google's ad teams constantly update filters that detect potentially malicious activity with intelligence from user-flagged ads, and will reverse-engineer fraud to pinpoint threat indicators. This process has allowed Google to build a significant repository of indicators and signals characteristic of threat actors. Google also uses automated "risk models" that scan ads to determine whether they are in violation of Google's ad policies.[38]

41. In recognition of their success, as measured by a third-party auditor, Google obtained the Trustworthy Accountability Group ("TAG")[39] Anti-Fraud Certification and Certificate against

[34] Nicholas Maida, *What is Malvertising?*, Cybersecurity & Information Systems Information Analysis Center (Dec. 17, 2018), https://csiac.org/articles/malvertising-explored/.
[35] *Advertising Fraud: How the Ad-Tech Industry is Tackling the Problem*, MIT Technology Review Insights (Dec. 15, 2014), https://www.technologyreview.com/2014/12/15/249612/advertising-fraud-how-the-ad-tech-industry-is-tackling-the-problem/.
[36] Darrell Etherington, *Google Acquires Spider.io To Help Spot And Stop Online Ad Fraud*, Tech Crunch (Feb. 21, 2014), https://techcrunch.com/2014/02/21/google-acquires-spider-io-to-help-spot-and-stop-online-ad-fraud/.
[37] *How does Google prevent invalid activity?*, Google Ads (last accessed Jan. 19, 2024), https://www.google.com/ads/adtrafficquality/how-we-prevent-it/.
[38] Sridhar Ramaswamy, *Making our ads better for everyone,* Google Public Policy Blog (Mar. 14, 2012), https://publicpolicy.googleblog.com/2012/03/making-our-ads-better-for-everyone.html
[39] Not to be confused with Google's own Threat Analysis Group, which the company founded in 2010 to counter government-backed cyber attacks. *Threat Analysis Group Official Blog*, Google (last accessed Jan. 12, 2024, https://blog.google/threat-analysis-group/; *Our cybersecurity journey through the years*, Google (last accessed Jan. 19, 2024), https://kstatic.googleusercontent.com/files/ba070caff65fa5331016c7720c9015346d564649ad822c704accd7538e3d4394f4ec2bf5e3250414f93d6b0e040cee34d4bd5c3bc3dc2dc1834f0fdc4bcae3bd.

Malware[40] as an intermediary, seller, and buyer, as well as TAG's Brand Safety Certification[41] as an intermediary and seller.[42] In 2017, TAG became the Information Sharing and Analysis Organization for the digital advertising industry, a Department of Homeland Security designation making TAG the primary forum for sharing threat intelligence in the industry.[43]

42. Google ad fraud prevention measures resulted in a substantial increase in the amount of malicious and fraudulent ads removed and ads violative of Google policies detected on and removed from its platform.

43. Since 2012, Google has issued annual Ads Safety and Quality Reports, describing its efforts at addressing ads safety and quality.[44] It was unusual in this time period for major industry participants to undertake and report out in this manner. A Google blog post introducing its 2022 Ads Safety Report describes an example of these efforts:

> Despite our continued efforts, bad actors increasingly operate at a greater scale and with more sophistication. They use a variety of tactics to evade detection. For example, at the end of 2022 and into the new year, we faced a targeted campaign of scammers creating thousands of accounts to spread malware by impersonating popular software brands. When we identify these coordinated threats, we urgently assess the situation and take action. In this example, we quickly identified how scammers are spreading their malware and put additional restrictions to block their ability to harm consumers. Over a one-month period, we blocked and removed tens of thousands of malicious advertisements and took action against the accounts associated with the bad ads.[45]

44. Bad ads are problematic for a number of reasons. For example, they disrupt the user experience on web pages with offensive or inappropriate content, abuse the ad network by promoting content that contains malware, and can otherwise contain prohibited or restricted content.

---

[40] *Certified Against Malware Guidelines Version 5.0*, The Trustworthy Accountability Group (last accessed Jan. 19, 2024), https://www.tagtoday.net/hubfs/CAM/TAG%20CAM%20Guidelines.pdf.
[41] *Brand Safety Certified,* The Trustworthy Accountability Group (TAG) (Jan. 2023), https://2848641.fs1.hubspotusercontent-na1.net/hubfs/2848641/BSC%20Version%202.1%20Final.pdf
[42] *Registry,* The Trustworthy Accountability Group (TAG) (last accessed Jan. 19, 2024), https://www.tagtoday.net/registry.
[43] *Trustworthy Accountability Group (TAG)*, The ISAO Standards Organization (last accessed Jan. 19, 2024), https://www.isao.org/group/tag/; *Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs)*, Department of Homeland Security Cybersecurity & Infrastructure Security Agency, (last accessed Jan. 19, 2024), https://www.cisa.gov/frequently-asked-questions-about-information-sharing-and-analysis-organizations-isaos.
[44] For example, *Ads Security: 2012 Retrospective*, Google Inside AdWords (Jan. 17, 2013), https://adwords.googleblog.com/2013/01/ads-security-2012-retrospective.html; *Busting Bad Advertising Practices – 2013 Year in Review*, Google Inside AdWords (Jan. 17, 2014), https://adwords.googleblog.com/2014/01/busting-bad-advertising-practices-2013.html.
[45] Alejandro Borgia, *Our 2022 Ads Safety Report*, Google Ads & Commerce Blog (Mar. 29, 2023), https://blog.google/products/ads-commerce/our-2022-ads-safety-report/.

45. The chart below depicts the number of bad ads removed by Google from 2014 to 2022, based on its Ads Safety and Quality Reports.[46]

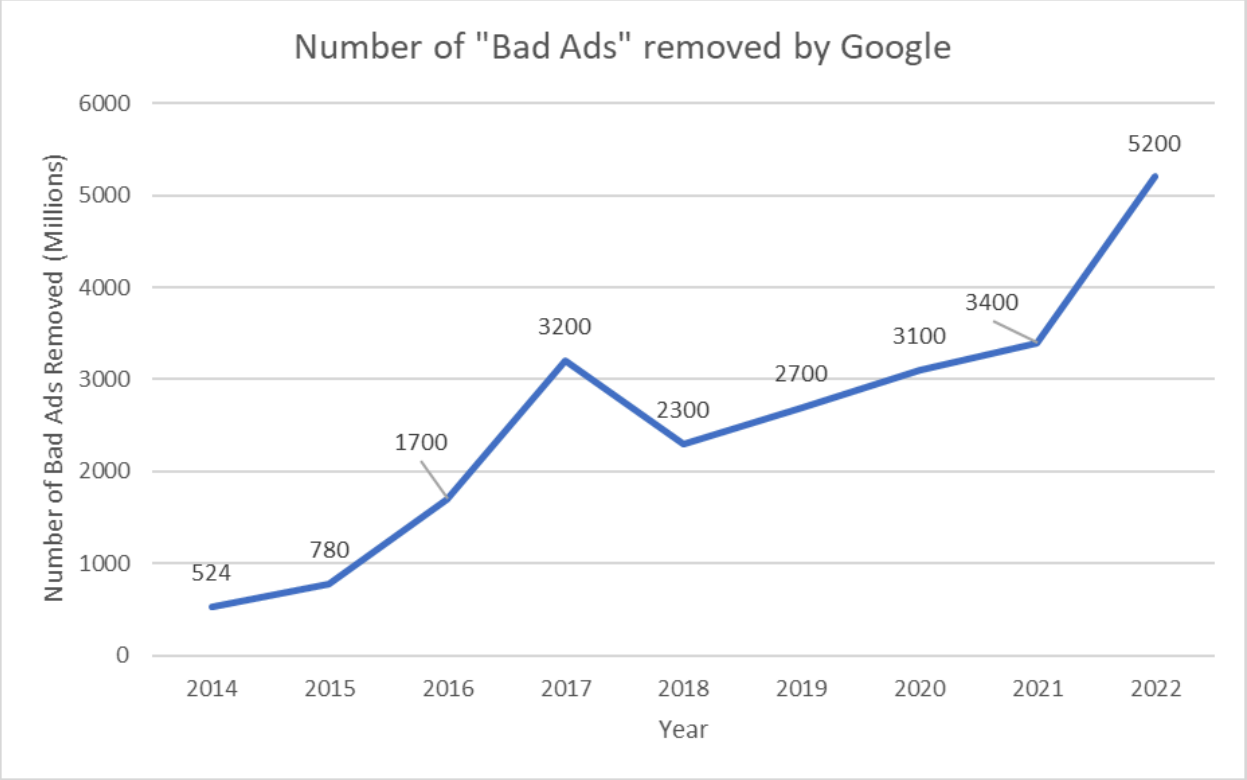


Figure E - Number of "Bad Ads" removed by Google

46. Google's policies are designed to support a safe and positive experience by prohibiting and restricting content and practices believed to be harmful to users and the overall advertising ecosystem. Prohibited content includes: the sale or promotion for the sale of counterfeit goods (e.g. a fake trademark or logo); the promotion of some products or services that cause damage, harm, or injury (e.g. recreational drugs); the promotion of products or services designed to enable dishonest behavior (e.g. hacking software or instructions); and ads or destinations that

[46] *Fighting Bad Advertising Practices on the Web — 2014 Year in Review*, Google Inside AdWords (Feb. 3, 2015), https://adwords.googleblog.com/2015/02/fighting-bad-advertising-practices-on.html; Sridhar Ramaswamy, *How we fought bad ads in 2015*, The Keyword (Jan. 21, 2016), https://blog.google/technology/ads/better-ads-report/; Scott Spencer, *How we fought bad ads, sites and scammers in 2016*, The Keyword (Jan. 25, 2017), https://blog.google/technology/ads/how-we-fought-bad-ads-sites-and-scammers-2016/; Scott Spencer, An advertising ecosystem that works for everyone, The Keyword (Mar. 14, 2018), https://blog.google/technology/ads/advertising-ecosystem-works-everyone/; Scott Spencer, *Enabling a safe digital advertising ecosystem*, Google Ads & Commerce Blog (Mar. 14, 2019), https://blog.google/products/ads/enabling-safe-digital-advertising-ecosystem/; *Keeping users safe on the ad-supported internet*, Google Safety Center (last visited Jan. 19, 2024), https://safety.google/stories/ads-safety-online/; *2020 Ads Safety Report*, Google (Mar. 17, 2021), https://services.google.com/fh/files/blogs/ads_safety_report_2020/; *2021 Ads Safety Report*, Google (May 4, 2022), https://services.google.com/fh/files/blogs/google_ads_safety_report_2021.pdf; *2022 Ads Safety Report*, Google (Mar. 29, 2023), https://services.google.com/fh/files/misc/2022_google_ads_safety_report.pdf.

display shocking content or promote hatred, intolerance, discrimination, or violence (e.g. hate group paraphernalia, ads using profane language). Google also restricts content such as pornography; ads or destinations that deceive users by excluding relevant product information or providing misleading information about products, services, or businesses; and more.[47] For a breakdown of Google's subcategories and the subsequent takedown of these "bad ads" by Google, see Appendix C.

47. As depicted in the chart below, the highest number of bad ads blocked or removed by Google in 2022, as violative of Google advertiser policies, involved users trying to "abuse the ad network" (1.36 billion).[48]

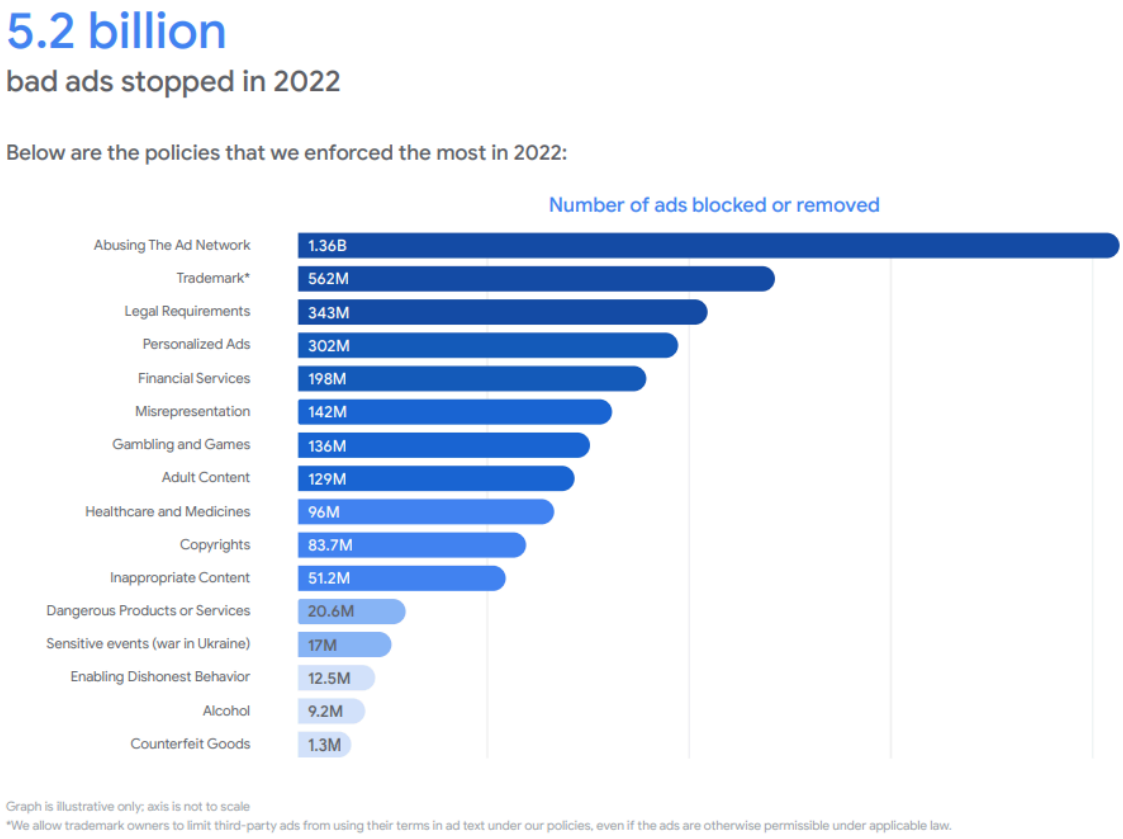


Figure F - Subcategories of Bad Ads Blocked or Removed by Google

[47] *Google Ads Policies,* Google Support Center (Dec. 2021), https://support.google.com/adspolicy/answer/6008942?hl=en.
[48] *2022 Ads Safety Report*, Google (Mar. 29, 2023), https://services.google.com/fh/files/misc/2022_google_ads_safety_report.pdf.

48. Google also enforces publisher policies that prohibit content that erodes trust in the advertising ecosystem, including malware embedded on publisher webpages. In 2022, Google took down 4.5 million web pages for violating Google's policy against including malware or unwanted software such as computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, or rogue security software, as indicated in the chart below.[49]

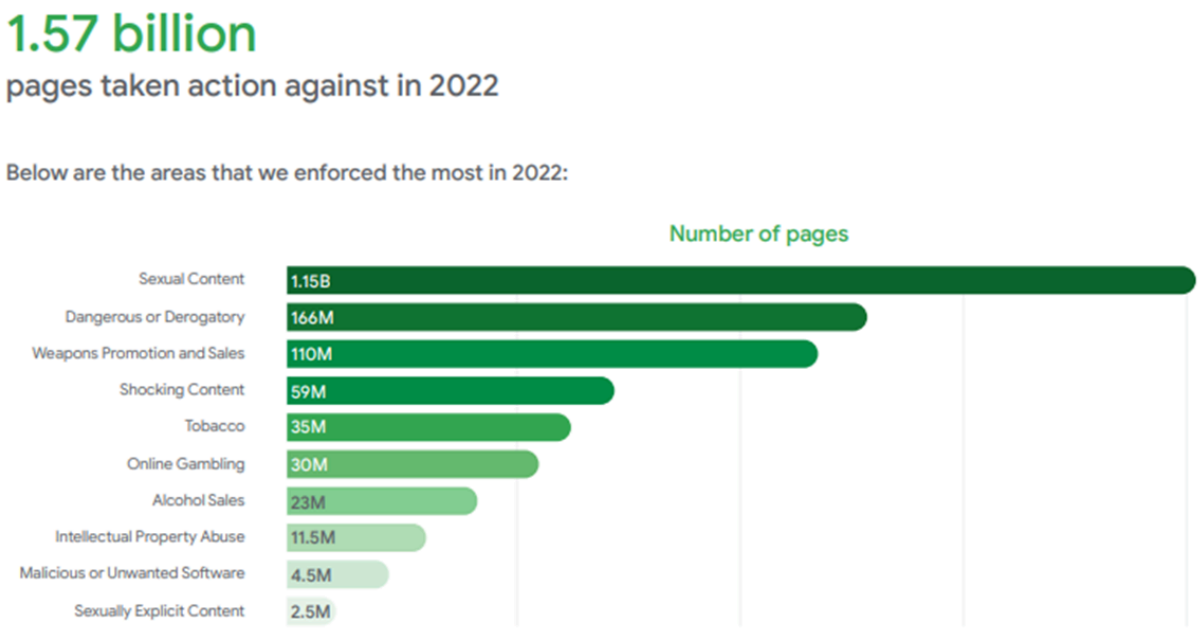


Figure G - Subcategories of Google Enforcement Actions on Publisher Pages

Google Has Played a Leading Role in Developing Industry Standards to Address Malvertising and Ad Fraud

49. Google has invested substantial amounts of time, money, and knowledge into the development of standards, tools, and industry working groups in order to bolster the security of the advertising ecosystem. Google has played a leading role in setting industry security standards as one of the first organizations to obtain TAG's anti-fraud certification, certification against malware, and brand safety certification, as well as through their involvement in the Interactive Advertising Bureau IAB Technology Laboratory ("IAB Tech Lab"), a global community of media companies, brands, and technology firms in the digital advertising space with a focus on brand safety, ad fraud, ad measurement, ad quality, and programmatic effectiveness.[50] Not only does Google's leadership in standard-setting organizations secure the advertising ecosystem, it encourages others in the industry to adhere to these standards as it allows other organizations

[49] *2022 Ads Safety Report*, Google (Mar. 29, 2023), https://services.google.com/fh/files/misc/2022_google_ads_safety_report.pdf; Publisher Policies Help, Google Publisher Policies: Malware or unwanted software, Google (last accessed Jan. 18, 2024), https://support.google.com/publisherpolicies/answer/10502938?sjid=8243386597193415776-NC&visit_id=638411902878675843-405821156&rd=1.

[50] *About the IAB Tech Lab*, IAB Tech Lab (last accessed Jan. 12, 2024), https://iabtechlab.com/about-the-iab-tech-lab.

to benefit from Google's security knowledge. The downstream effects from shared security knowledge and tools through cooperation with industry partners and working groups has a beneficial impact on all parties involved.

50. Google developed the ads.txt file and worked with IAB Tech Lab to make it an industry standard to combat fraudulent and malicious actors, with an emphasis on finding a way to combat domain spoofing, hijacking, and illegitimate ad inventory. The IAB Tech Lab publicized the first iteration of ads.txt in May 2017 in conjunction with a report co-authored by a Google engineer and consultant.[51]

51. An ads.txt file is an "authorized digital seller" text file added to a publisher's domain so that advertising platforms can verify inventory and publisher relationships. Ads.txt files contain details on all of the programmatic advertising affiliates (i.e., supply side channels, ad networks and ad exchanges) where a publisher operates with their site server.[52] Marketers can use the ads.txt file to verify that the seller account ID corresponds to the ID within the ads.txt file. If they do not align, it may mean that the website does not come from an authorized digital seller or that the seller is not authorized to sell ads, increasing the transparency of a publisher's inventory by revealing where impressions are purchased and sold. Ads.txt also allows publishers to declare which companies are authorized to sell their inventory.

52. Ads.txt played an instrumental role in diminishing domain spoofing exacerbated by the growth of header bidding.[53] As explained in detail below, the server-to-server connections involved in header bidding prevented exchanges from independently verifying the true URL of an ad request in real time. The ads.txt industry standard raised the security bar against bad actors whether they ran through header bidding or Google's Open Bidding technology.

Google Detected and Played a Leading Role in the Takedown of 3ve, Collaborating with White Ops, the FBI, and Industry Participants

53. One of the most massive and complex fraud operations in digital advertising was an ad fraud threat actor group 3ve (pronounced "Eve") that, through three sub-operations, forged fake ad traffic from bots, as well as fake publisher inventory. Google and White Ops (a bot-detection firm, now known as HUMAN Security) independently detected 3ve and then worked together to analyze the 3ve operations, including the identification of the three sub-operations and the malware associated with the spread of the operation's botnets, which was facilitated with the assistance of ProofPoint and MalwareBytes. At its peak, 3ve generated between 3 billion and 12 billion or more daily ad bid requests.[54] Google and White Ops presented to the FBI the results of

[51] *AB Tech Lab Authorized Sellers for Apps (app-ads.txt)*, IAB Tech Lab (Mar. 2019), https://iabtechlab.com/wp-content/uploads/2019/03/app-ads.txt-v1.0-final-.pdf.
[52] *Ads.txt for Publishers*, Publift (Jun. 12, 2023), https://www.publift.com/blog/ads-txt-for-publishers.
[53] Sarah Sluis, *How Ads.txt Took Down 3ve, As The FBI Took Down Its Creators*, Ad Exchanger (Dec. 3, 2018), https://www.adexchanger.com/online-advertising/how-ads-txt-took-down-3ve-as-the-fbi-took-down-its-creators/; Ross Benes, *Blast from the past: Why old ad fraud tactics won't die*, Digiday (Oct. 30, 2017), https://digiday.com/marketing/blast-past-old-ad-fraud-tactics-wont-die/.
[54] *The Hunt for 3ve* at Page 7, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.

their investigation and, together with the FBI and ultimately other industry participants, took down 3ve.

54. As a whole, the 3ve operation utilized domain spoofing in order to make fraudulent websites appear as legitimate and reputable websites, which can be difficult for ad exchanges to identify on their own. 3ve would then sell this fake publisher inventory to advertisers. Once sold to an advertiser, the bad actors would direct their various botnets to the fake websites, generating fraudulent ad impressions. These impressions would then fraudulently inflate the price of bid requests on 3ve's spoofed domains, allowing them to sell inventory at a higher price. This botnet was able to maintain success and avoid detection due to the sophistication and various approaches of 3ve's sub-operations.

55. The first 3ve sub-operation, 3ve.1, consisted of a few bot networks operating from data centers across the U.S. and Europe. Even though significant traffic originated from the same few locations, 3ve.1's operations were difficult to detect because they utilized a series of proxies through border gateway protocol ("BGP") hijacks[55] and compromised malware-infected devices to appear as if they were originating from a variety of residential and business devices.[56] The data centers located in the U.S. and Europe acted as the Command and Control centers which, upon command, would initiate the botnet's operations and send ad requests with the appearance that they originated from a variety of residential and business devices. Over time, the 3ve.1 botnet evolved not only to appear as if it originated from residential and business computers, but also from mobile Android devices, further obfuscating the malicious activity.

56. The second operation, 3ve.2, used spoofed domains to sell fake ad inventory to advertisers. While 3ve.1 used proxy devices and IPs to obfuscate its activity, 3ve.2 utilized a "custom-built browsing engine, installed with the Kovter[57] botnet, which had infected hundreds of thousands of computers through malvertising campaigns."[58] 3ve.2's browser would be used to visit spoofed domains in order to generate fake ad impressions. In circumstances where a video ad may have been shown on the spoofed website, the botnet had the capability to play media, in order to generate further impressions on each site it visited. 3ve.2 used additional methods to obfuscate its activity including hidden windows to hide the activity from end users; fake browsing and random mouse movement to emulate a legitimate end user; tag evasion, the process of blocking ad fraud detection tools or any other unwanted script that would detect malicious ads from executing; non-spoofed domain browsing, the process of visiting legitimate domains; and geographic locations where ad networks would expect organic users to visit from.

57. The third operation, 3ve.3, was very similar to 3ve.1 in that it used data centers to host its bot networks. However, instead of using proxy devices, 3ve.3 used other data center IP addresses to

[55] BHP hijacking is when malicious actors reroute Internet traffic through announcing false ownership of groups of IP addresses, called IP prefixes, that they do not actually own, control, or route to.
[56] *The Hunt for 3ve* at Page 11, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.
[57] Kovter is a trojan malware that is typically distributed via email attachments.
[58] *The Hunt for 3ve* at Page 12, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.

attempt to obfuscate its activity. While the use of data centers is much easier to detect by ad filters, data centers provide a far greater bandwidth and 3ve.3's malicious activity could be conducted in a more effective manner. Whenever a data center was detected and its traffic was restricted, 3ve.3 could find a new data center to compromise and utilize. All of these components of the operation exploited various aspects of the digital ad exchange ecosystem, and would require a holistic response to shut it down.

58. The 3ve operation was massively destructive in scale. Using thousands of servers simulating human activity, three to twelve billion ad bid requests were generated daily; about 1.7 million PCs were infected with malware to falsify billions of ad views; 700,000 active desktop infections occurred at any given time; one million IP addresses were compromised; approximately 10,000 websites were created to impersonate legitimate web publishers; and over 60,000 accounts were selling fake ad inventory to digital advertising companies.[59] As a result of the 3ve.2 sub-operation alone, it has been estimated that publishers paid over $29 million USD to the fraudsters between January 2016 through May 2017 for ads that no human ever saw.[60]

59. Due to the sophisticated techniques employed, as well as a sudden increase in operational scale, Google and White Ops gathered enough evidence to refer the case and findings to federal law enforcement in 2017. As Google and White Ops worked to secure ad system traffic from the 3ve operations, they identified partners in the industry who had also observed and were victimized by the operations, and formed a secret coalition of roughly 17 cybersecurity, advertisement technology, Internet and security companies, as well as federal law enforcement.[61] Google and White Ops founded this working group in order to ensure the success of a full takedown of the 3ve operations and minimize 3ve's ability to simply "move" or alter their operations through the use of alternative IP addresses and botnets. The secret coalition of private and federal entities dedicated months to strategizing and coordinating a technical takedown of 3ve's infrastructure in order to block the operators from being able to rebuild.[62] The other organizations in the coalition included Adobe, Trade Desk, Amazon, Oath, Malwarebytes, ESET, Proofpoint, Symantec, F-Secure, McAfee, and Trend Micro. Each company had its own unique role, with White Ops, Google and law enforcement leading the overall effort.[63]

60. Just within Google and White Ops, there were over 30 people involved across the two companies, including software engineers, security researchers, threat analysts, project

---

[59] *The Hunt for 3ve* at Pages 3 and 10, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf; Craig Silverman, *8 People are Facing Charges as a Result of the FBI's Biggest-Ever Ad Fraud Investigation,* BuzzFeed News (Nov. 27, 2018), https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown.

[60] Indictment at Paragraph 39, *United States* v. *Zhukov et al.*, Case No. 18-633 (E.D.N.Y. Nov. 27, 2018).

[61] *The Hunt for 3ve* at Pages 3 and 14, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf; *Industry collaboration leads to takedown of the "3ve" ad fraud operation*, Google Security Blog (Nov. 27, 2018), https://security.googleblog.com/2018/11/industry-collaboration-leads-to.html.

[62] *Industry collaboration leads to takedown of the "3ve" ad fraud operation*, Google Security Blog (Nov. 27, 2018), https://security.googleblog.com/2018/11/industry-collaboration-leads-to.html.

[63] *The Hunt for 3ve* at Page 4, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.

managers, product managers, data scientists, publicists, and lawyers. The core research team would meet on a weekly basis to share findings, indicators of compromise, and coordinate the work for the following week.

61. While the coalition was able to develop a means of identifying some of the traffic originating from the 3ve botnet, such as those employed by 3ve.3, the various means by which the botnet was deployed meant that, even when the associated IP addresses and traffic were blocked, the 3ve operators could have the botnet up and operable again in little to no time. As a result, the coalition dedicated its time to dissecting the 3ve campaign's tactics, from the malware used to deploy the botnet, the spoofed domains used to inflate prices, and understanding the full scope and extent of assets utilized by the campaign. While the team was strategizing the takedown of 3ve, they had to allow the fraudsters to continue to earn some revenue to avoid tipping off 3ve's operators that they had been discovered. Google allowed 3ve's counterfeit websites to earn revenue through its ad systems but later refunded those who lost money on ads that ran.[64]

62. On November 27, 2018, Google, White Ops, the FBI, DHS, and other organizations in the coalition initiated the takedown of 3ve operations by using their findings to target and restrict traffic from the operation's critical infrastructure and data centers, "freeing" compromised devices, removing counterfeit websites, and seizing in-use servers and domains. Within 18 hours of the counter-operations beginning, incoming bot traffic from 3ve was reduced to near-zero.[65]

[64] Craig Silverman, *8 People Are Facing Charges As A Result Of The FBI's Biggest-Ever Ad Fraud Investigation*, Buzzfeed News (Nov. 27, 2018), https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown.

[65] *The Hunt for 3ve* at Pages 14-15, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf; Jeff Beer, *FBI and Google take down multimillion-dollar ad fraud operation*, Fast Company (Nov. 28, 2018), https://www.fastcompany.com/90273549/fbi-and-google-take-down-multi-million-dollar-ad-fraud-operation.

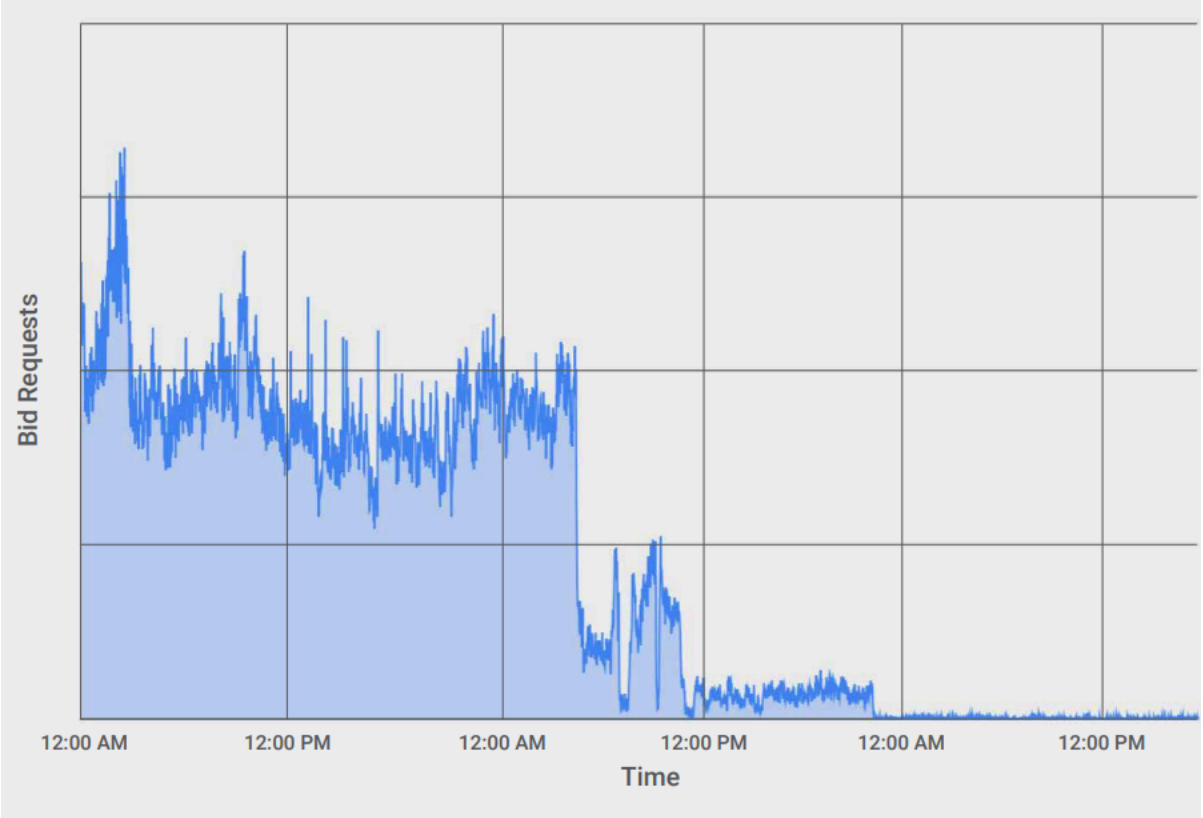


Figure H: Incoming 3ve.2 bid requests on November 27 and 28

63. As part of the efforts, the FBI seized 31 domains, information from 89 computer servers, and multiple international bank accounts associated with the schemes.[66] On November 28, 2018, a 13-count indictment was unsealed targeting eight actors from the 3ve operations.[67] The entire takedown process of 3ve was a nearly two-year operation, but the recovery of proceeds continued through 2022, when the U.S. government announced that it had recovered over $15 million in proceeds from the 3ve ad fraud operation that cost businesses more than $29 million. This forfeiture is the largest international cybercrime recovery in the history of the Eastern District of New York.[68]

---

[66] Craig Silverman, *8 People Are Facing Charges As A Result Of The FBI's Biggest-Ever Ad Fraud Investigation*, Buzzfeed News (Nov. 27, 2018), https://www.buzzfeednews.com/article/craigsilverman/3ve-botnet-ad-fraud-fbi-takedown.

[67] Press Release, *Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud*, U.S. Attorney's Office, Eastern District of New York (Nov. 27, 2018), https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing.

[68] Press Release, *United States Recovers Over $15 Million from Swiss Bank Accounts as Proceeds of Global Digital Advertising Fraud Scheme*, U.S. Attorney's Office, Eastern District of New York (May 18, 2022), https://www.justice.gov/usao-edny/pr/united-states-recovers-over-15-million-swiss-bank-accounts-proceeds-global-digital.

64. The identification and subsequent shut down of the 3ve operations led to significant developments and improvements within the digital advertising space that bolstered security and the quality of advertisements. The 3ve campaign highlighted substantial issues concerning the use of spoofed domains and how the use of spoofed domains resulted in substantially inflated prices from fraudulent ad traffic, allowing threat actors utilizing this tactic to benefit financially with a substantial impact on legitimate advertisers. One of the more effective ways of combating domain spoofing and validating that an advertisement belongs to a reputable publisher is through the use of the previously discussed "ads.txt" files.

65. As set forth in Google and White Ops' whitepaper on the 3ve operation, 80% of the traffic from 3ve was unauthorized, or was "offered for sale by sellers that were not listed as authorized sellers in a domain's ads.txt file."[69] Had ads.txt been adopted and enforced by advertisers at 3ve's inception, most of the unauthorized traffic may have been blocked. Another study, conducted and published by the Association of American Advertisers (ANA) and White Ops in May of 2019, projected an 11% decrease in losses resulting from ad fraud in 2019, primarily attributable to the implementation of ads.txt, the requirement that ads.txt be used in order to become TAG ad fraud certified, and the arrests of those involved with the 3ve and Methbot operations.[70]

[69] *The Hunt for 3ve* at Page 16, Google and White Ops (Nov. 2018), https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf.

[70] Press Release, *Report From ANA And White Ops Shows War On Ad Fraud Is Succeeding*, the Association of National Advertisers (May 1, 2019), https://www.ana.net/content/show/id/pr-2019-war-succeeding#:~:text=The%20monetary%20losses%2C%20while%20significant,percent%20between%202017%20and%202019.

Header Bidding

The Rise of Header Bidding Created Additional Opportunities for Fraudulent Activity, Largely in the Form of Domain Spoofing

66. Header bidding is a programmatic auction in which publishers send bid requests to multiple demand partners in real time outside of their primary ad server. It became widely adopted by publishers in 2014 and 2015, before ads.txt was developed and became an industry standard.

67. Header bidding works through JavaScript code placed in the header part of the publisher's website's page, known as a header bidding wrapper, that manages the demand partners participating in the auctions, whether they be supply-side platforms ("SSPs"), demand-side platforms ("DSPs"), or ad networks. The header bidding code collects bids from every partner before closing the sale. Publishers are able to set price floors, manage demand partners, and configure auction time limits to reflect their marketing goals over time. Publishers can engage in header bidding either through open-source wrappers run by in-house developers or by hiring a third-party header bidding provider.

68. While header bidding gave publishers a way to connect directly with advertisers, the technology introduced security vulnerabilities that bad actors can, and often do, exploit. These vulnerabilities included: (1) an inability to prevent fraud amongst the "noise" of multiple calls; (2) a lack of guardrails to protect against malvertising; and (3) user and publisher data leakage.

Inability to Prevent Ad Fraud Among the "Noise"

69. The sheer multitude of bid requests involved in header bidding makes it harder for publishers to catch ad fraudsters in the act. Publishers who use header bidding want their demand partners to access their inventory under multiple bidding scenarios and through multiple demand partners. On average, the top 100 publishers (in terms of comScore traffic) have four header bidding partners (a header bidding partner is a source of demand for ad inventory such as a network that the header bidding wrapper is programmed to send calls to when a user visits a website).[71] Further, 45% of publishers utilize more than one header wrapper, which gives bad actors more points of entry to take advantage of.[72]

70. The technical complexities of implementing header bidding, in conjunction with publishers becoming more willing to add demand partners in the hopes of increasing their revenue, generated increased noise in bid requests where threat actors could hide.[73] As IAB Tech Lab Chief Technical Officer Sam Tingleff explained: "Header bidding led to publishers being more

[71] Ross Benes, *Unraveling header bidding's problems with user data*, Digiday (Mar. 20, 2017), https://digiday.com/media/header-bidding-security/.
[72] Alisha Rosen, *A Publishers Guide to Header Bidding and Ad Quality*, Headerbidding (Dec. 30, 2023), https://headerbidding.co/header-bidding-and-ad-quality/.
[73] Sarah Sluis, *How Ads.txt Took Down 3ve, As The FBI Took Down Its Creators*, Ad Exchanger (Dec. 3, 2018), https://www.adexchanger.com/online-advertising/how-ads-txt-took-down-3ve-as-the-fbi-took-down-its-creators/#:~:text=When%20publishers%20adopted%20Ads.,White%20Ops%20CTO%20Tamer%20Hassan.

promiscuous in their demand partnerships, and more willing to turn on demand partners, which made it easier for bad actors to hide amongst all the activity."[74]

71. The noise of multiple bid requests in header bidding also made it difficult for advertisers to identify and prevent domain spoofing. As the volume of bid requests rose, it in turn became difficult for advertisers to understand where the inventory was coming from due to the various parties involved and greater strain on the humans tasked with investigating fraudulent activity at DSPs, often without advanced traffic quality technology.[75] This created a security gap that threat actors were able to exploit through domain spoofing. As explained above, domain spoofing occurs when a fraudulent website or ad network sells an impression on a legitimate, reputable site, even though the impression will actually be served on an unknown site with lower quality (or bot) traffic. Buyers are misled into thinking that the legitimate site delivered poor results since these low-quality impressions perform much worse than the premium inventory they imitate. The lack of transparency into inventory allowed threat actors to send botnets to spoofed domains, subsequently to trigger bid requests for ads on these pages, and funnel ad revenue into their bank accounts.[76]

Lack of Guardrails Against Malvertisers

72. Header bidding further opened publishers to the threat of malvertising as publishers' desire to increase their revenue led to the regular adding and switching of partners to find which ones provided the highest ad revenue. Prior to the development of the header bidding methodology, most auctions followed the waterfall method, in which a publisher typically started by trying to sell its inventory via direct sales, which typically yielded the highest CPMs.[77] If it was unable to do so, the impression would be passed down to various ad networks until it was sold. The waterfall method allowed for a layer of security, as the order in which it offered impressions to SSPs, DSPs or networks was predetermined by the publisher and typically based on their historical performance for the publisher. As such, those demand partners prioritized in the chain were typically more reputable and less likely to conduct malicious activity. Further, as the waterfall method offered the impression to one partner at a time and in a predetermined manner, it was significantly easier to identify which advertisers were being offered the impressions and the participants in the process.

73. With header bidding, there was a lack of guardrails and standards for entry and participation, therefore making it easier for threat actors, whose tactics include malvertising, to enter and

[74] Sarah Sluis, *How Ads.txt Took Down 3ve, As The FBI Took Down Its Creators*, Ad Exchanger (Dec. 3, 2018), https://www.adexchanger.com/online-advertising/how-ads-txt-took-down-3ve-as-the-fbi-took-down-its-creators/.

[75] *Why publishers need to protect their reputations in the age of server-to-server*, Digiday (Jun. 16, 2017), https://digiday.com/sponsored/openxsbl-005-why-publishers-need-to-protect-their-reputations-in-the-age-of-server-to-server/.

[76] Press Release, *3ve – Major Online Ad Fraud Operation*, Department of Homeland Security Cybersecurity and Infrastructure Security Agency (Nov. 27, 2018), https://www.cisa.gov/news-events/alerts/2018/11/27/3ve-major-online-ad-fraud-operation.

[77] CPM (cost per mille) is a paid advertising option where companies pay a price for every 1,000 impressions an ad receives.

participate in header bidding auctions. Google previously saw the impact of a lack of guardrails and standards for entry of participation with its AwBid program, which allowed advertisers that used Google Ads to bid on third party exchanges. However, by allowing advertisers to bid on third party exchanges, the ads were not subject to the policies and tooling mechanisms Google had in place to examine ads and inventory on its own AdX exchange.[78] In 2013, Google's research noted that the spam click rate through AwBid varied anywhere from 10 to 70% while AdX remained at 7 to 8%.[79] This comparison of and view of spam rates through AwBid (outside exchanges) compared to AdX and advertisers bidding within the Google ad exchange shows the benefits of Google's security mechanisms and policies.

Data Leakage

74. Data leakage is the unauthorized passage or transmission of typically non-public or sensitive data from inside an organization or system to a destination outside of its intended network. Leaked data is generally information that an organization or individuals do not intend to make public, such as business and financial information or personal identifiable information. Publishers share the following user information with multiple third parties when they run bidding on open source code on their webpages: user's IP address, user's cookie, user's browser, domain and URL of the page, previous page loaded by the user, publisher shared data on the user (e.g., gender, race, parent, income bracket, education, year of birth, zip code), and potential specific data on interests (e.g., movie bug, fitness enthusiast, pet lover). Each and every bidder receives the data about the users who will be served an ad, leading to multiple opportunities for data leaks.

75. The emergence of header bidding introduced various security concerns regarding data leakage as a result of the simultaneous manner in which calls are sent to bidders. The simultaneous call outs allow bidders to view the data from each user who was served an impression in an auction. In these instances, the header bidding call out will include relevant information about the Internet user for bidders to make a determination on whether they want to bid on the ad. As the bid request is sent to all partners, each bidder can get access to the data from every impression. Buyers can very easily abuse the system by "listening" for data without spending any money by simply receiving bid requests without the intention of winning the auction, allowing the buyers to sift through the publisher's data, even if they do not intend to win the auction. Further, some exchanges allow demand-side platforms to take bid requests and "listen" for data without spending money, leading to even more parties involved that may have access to a user's data. This has repercussions on both the users involved as well as publishers. Data leakage may impact and devalue publisher inventory, as a result of re-targeters using audience data from premium publishers to target their users, while visiting websites that have lower CPMs. With regards to users, it may be an annoyance, from the publication of non-public user information or, in extreme scenarios, this information may lead to malicious actors compromising their personal accounts and devices.[80]

[78] GOOG-DOJ-13249608.
[79] GOOG-AT-MDL-012551468.
[80] Ross Benes, *Unraveling header bidding's problems with user data*, Digiday (Mar. 20, 2017), https://digiday.com/media/header-bidding-security/.

Google's Open Bidding Technology

76. One of the more significant factors leading to ad fraud is an exchange's distance and lack of relationships with ad sellers, which positions them far removed from the actual source of impressions they sell.

77. In 2016, Google introduced Open Bidding (also referred to as Exchange Bidding), a programmatic advertising solution that allows publishers to invite external ad exchanges, SSPs, and networks to compete in a unified auction alongside Google AdX for ad inventory on their website. In contrast with header bidding, Google's Open Bidding technology provides bidding over Google's servers, as opposed to through code embedded in the publisher's page. Open Bidding requests occur through a server-to-server integration between publishers and demand partners. The server-to-server integration means that, instead of bidding through page tags and via browsers on the user's device, bidding takes place on the ad server, resulting in increased security, reduced latency for end users, easier implementation for web developers, less complicated communication between DSPs and SSPs, and easier maintenance and configuration.

78. Google's integrated approach gives Google control over the data flowing through its platform. This control allows Google to implement data privacy measures designed for the responsible management of user data, subject to quality policies and restrictions. These policies and restrictions include, for example, the prohibition of: misleading and dishonest ads, such as malware or the sale of illegal or counterfeit products; dangerous content; and interfering ads, such as those that require interaction with the ad to visit the page.[81]

[81] *Google Publisher Policies*, Google Ad Manager Help (Jan. 12, 2014), https://support.google.com/admanager/answer/10502938?sjid=16490059553950075395-NA&visit_id=638338563923173707-954928084&rd=1; Google Publisher Restrictions, Google Ad Manager Help (Jan. 12, 2014), https://support.google.com/admanager/answer/10437795?hl=en&ref_topic=7316904&sjid=16490059553950075395-NA%20; *Google Ad Manager Partner Guidelines,* Google Ad Manager Help (last accessed Jan. 12, 2024), https://support.google.com/admanager/answer/9059370?hl=en.

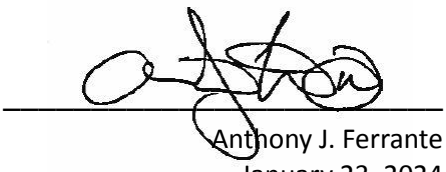
Conclusion

79. As the use of digital advertising has grown, opportunities for–and the magnitude of–malvertising and advertising fraud have likewise grown, with more than $100 billion in losses to the digital advertising ecosystem worldwide projected in 2024. Malvertising and ad fraud have been, and will continue to be, a significant issue for all Internet users as a result of the benefits and prevalence of the overall digital advertising ecosystem. As such, it is critical to ensure the digital advertisement space is as safe and secure as possible.

80. Google has engaged in efforts to create a safer and more secure digital advertising ecosystem for all participants. Google, for example, made substantial investments into the development of mechanisms, tools, and processes to fight the rising threat of malicious ad activity, including working with industry working groups such as the IAB Tech Lab and TAG to develop quality and security standards across the industry for the benefit of all digital advertisers, and providing dedicated and experienced personnel and assets to respond to and address cybersecurity threats and risks both proactively and reactively, as seen with 3ve. Google's investments, tools, teams, and collaboration with the industry, such as those efforts through TAG and IAB, can ensure a better and safer user experience for all parties using the Internet.

81. The open environment in which header bidding operates, and header bidding's lack of integration between exchanges and its participants, lead to ample opportunity for malicious actors to take advantage of Internet users and advertisers. Google's development of Open Bidding as an alternative to header bidding allowed for Google to apply and provide its internally developed tools, resources, skills, and intelligence to all stakeholders and participants within its advertising ecosystem in an integrated environment, enabling Google to bolster security through the application of its tools and standards at all ends of the process.

82. Google has proven itself to be a pioneer in protecting all players in the advertising space - from consumers to publishers to advertisers - and invests in the best resources and technology to achieve that goal. Google could have stood by and done nothing and let crime and fraud proliferate, but they took the actions that they did to the benefit of the entire online ecosystem.



Anthony J. Ferrante
January 23, 2024

Appendix C: "Bad Ads" Takedown Subcategories

Google's 2020, 2021, and 2022 Ad Safety Reports list categories of "bad ads" removed year after year. The following graphs demonstrate that Google consistently removed a high volume of bad ads for Adult Content, Inappropriate Content, Misrepresentation, Enabling Dishonest Behavior, Dangerous Products or Services, Counterfeit Goods, and Abusing the Ad Network in recent years.

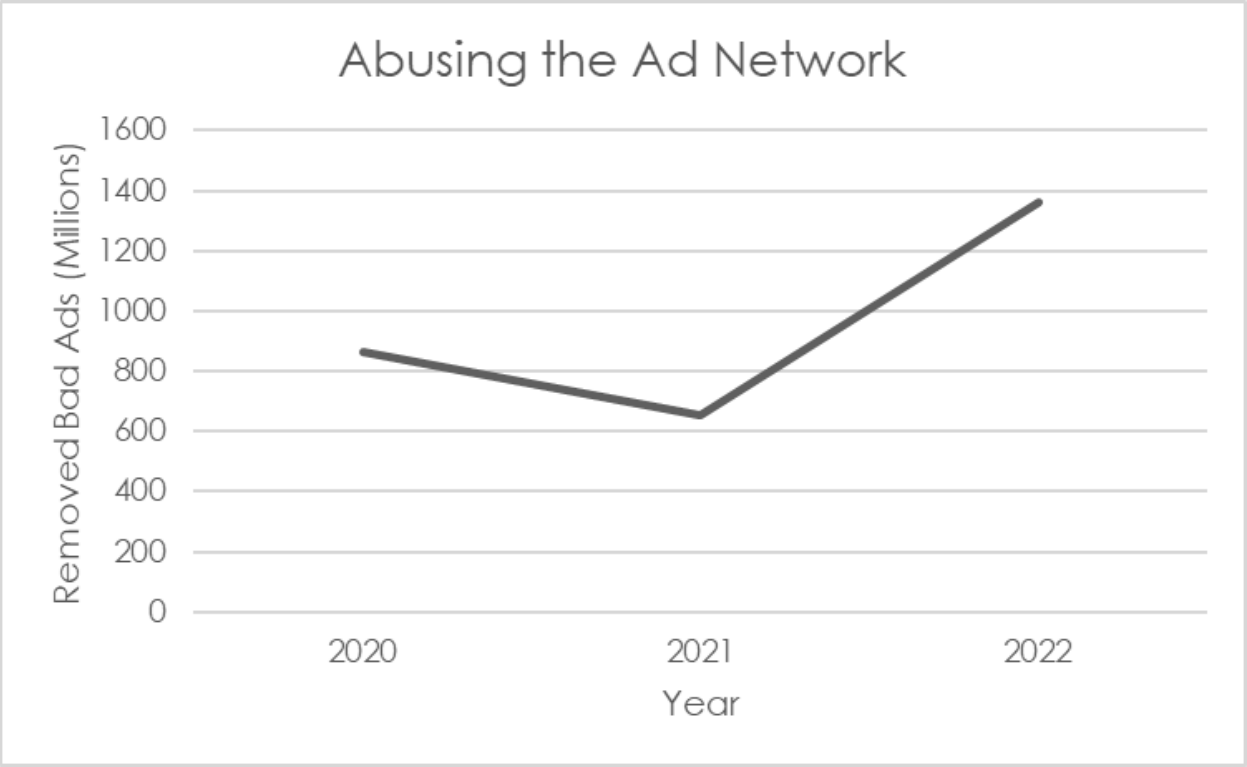


Figure I - Subcategory of Bad Ads Blocked or Removed by Google

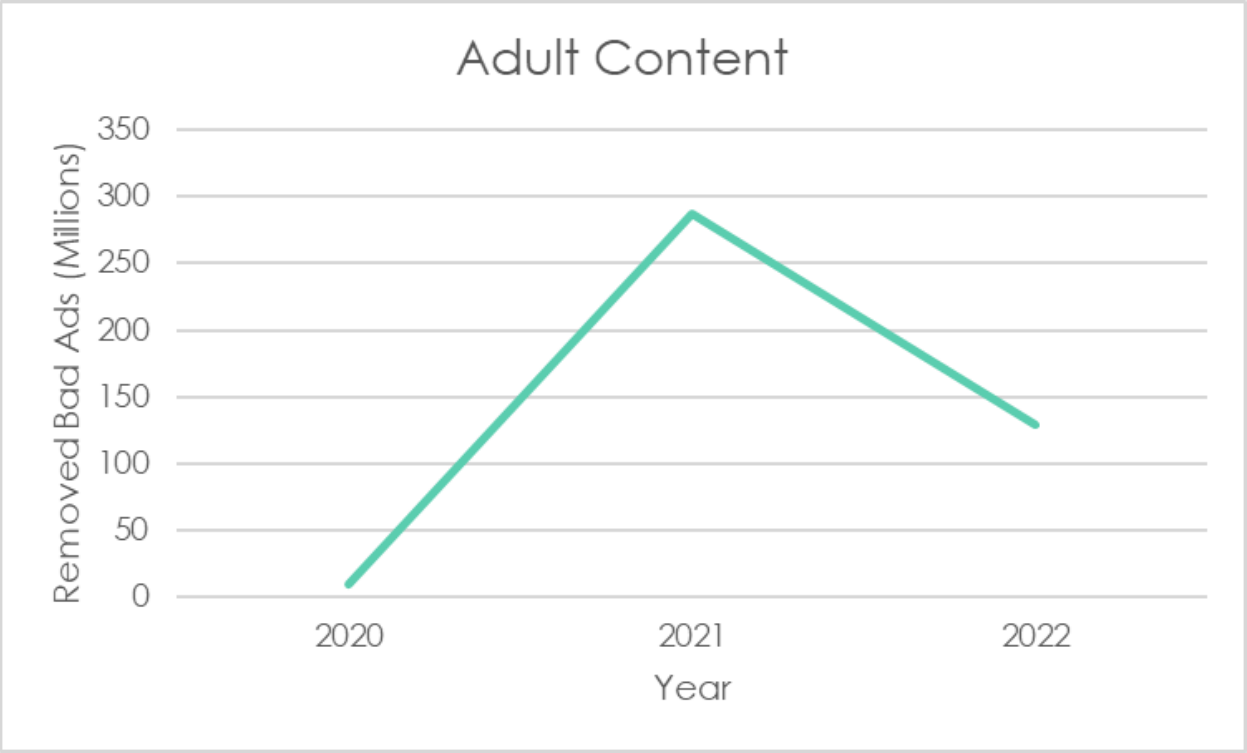


Figure J - Subcategory of Bad Ads Blocked or Removed by Google

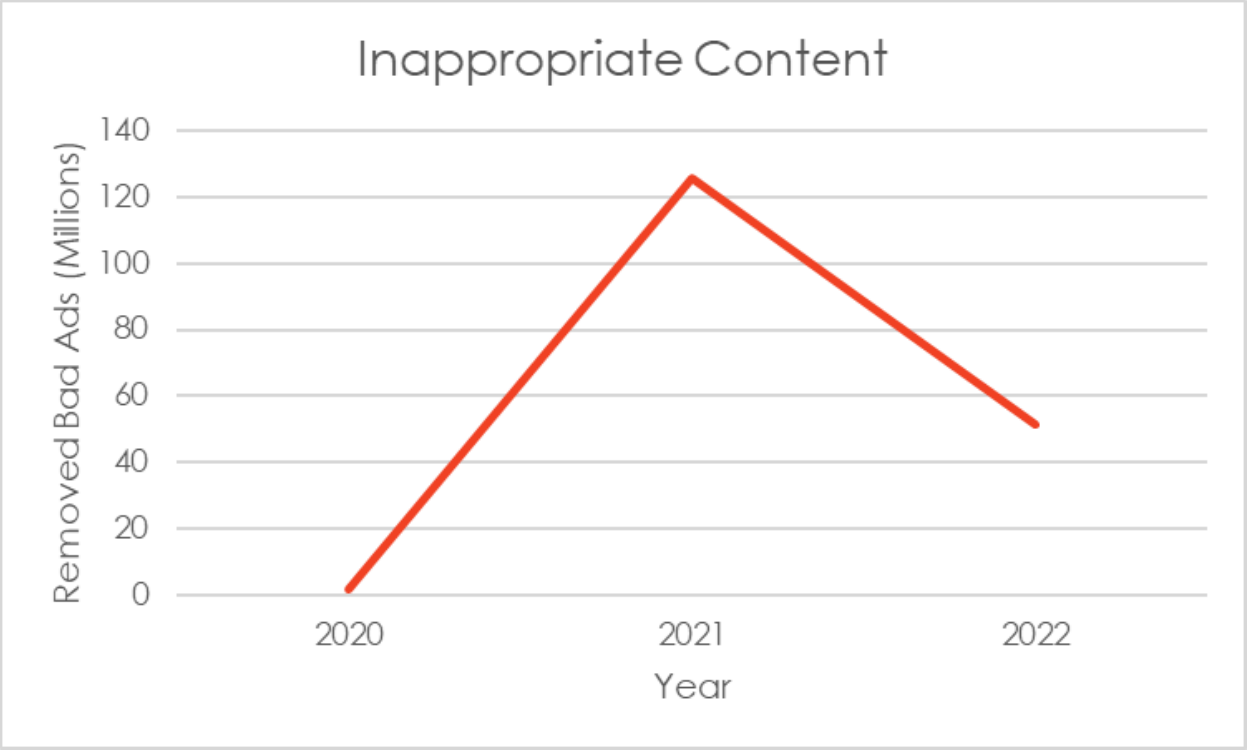


Figure K - Subcategory of Bad Ads Blocked or Removed by Google

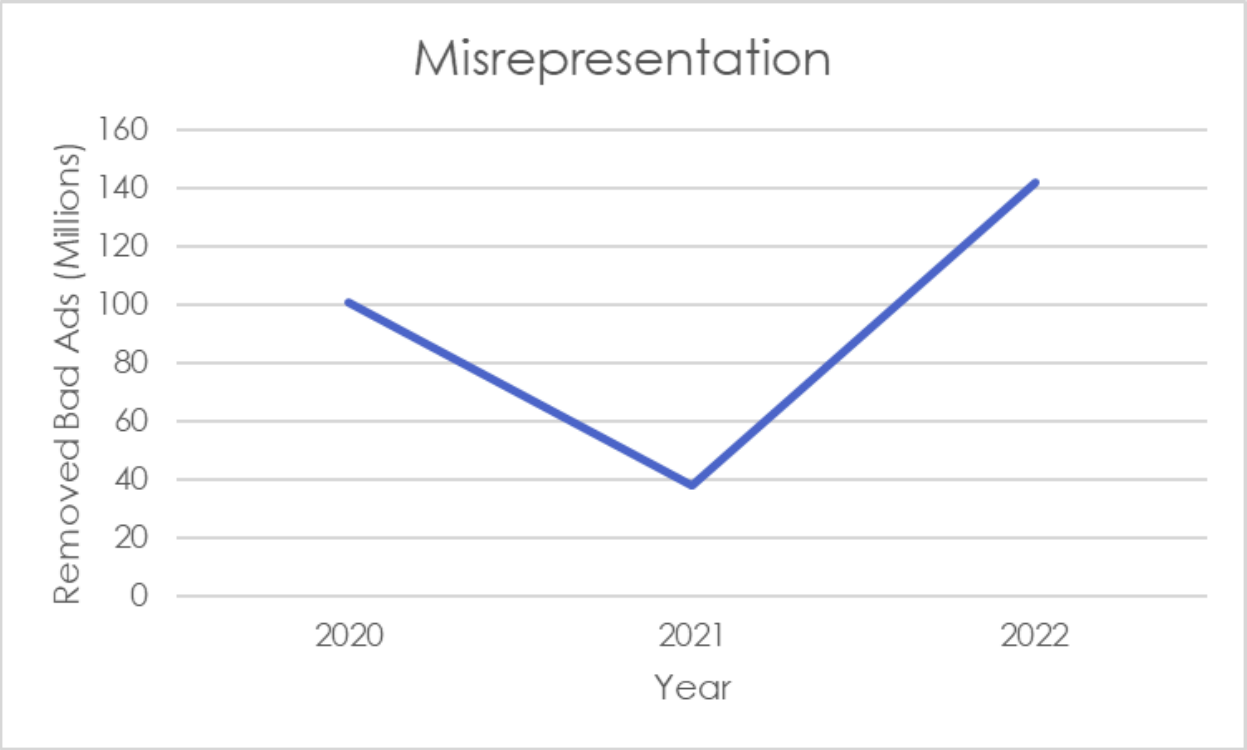


Figure L - Subcategory of Bad Ads Blocked or Removed by Google

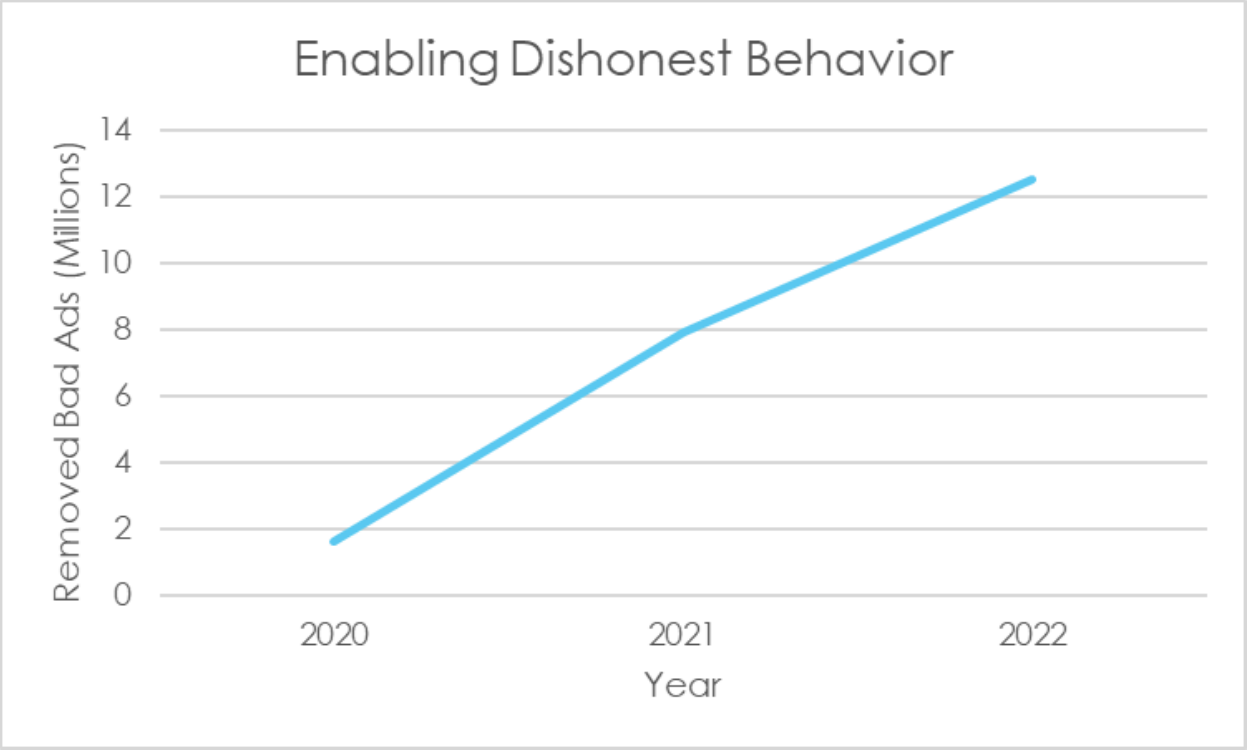


Figure M - Subcategory of Bad Ads Blocked or Removed by Google

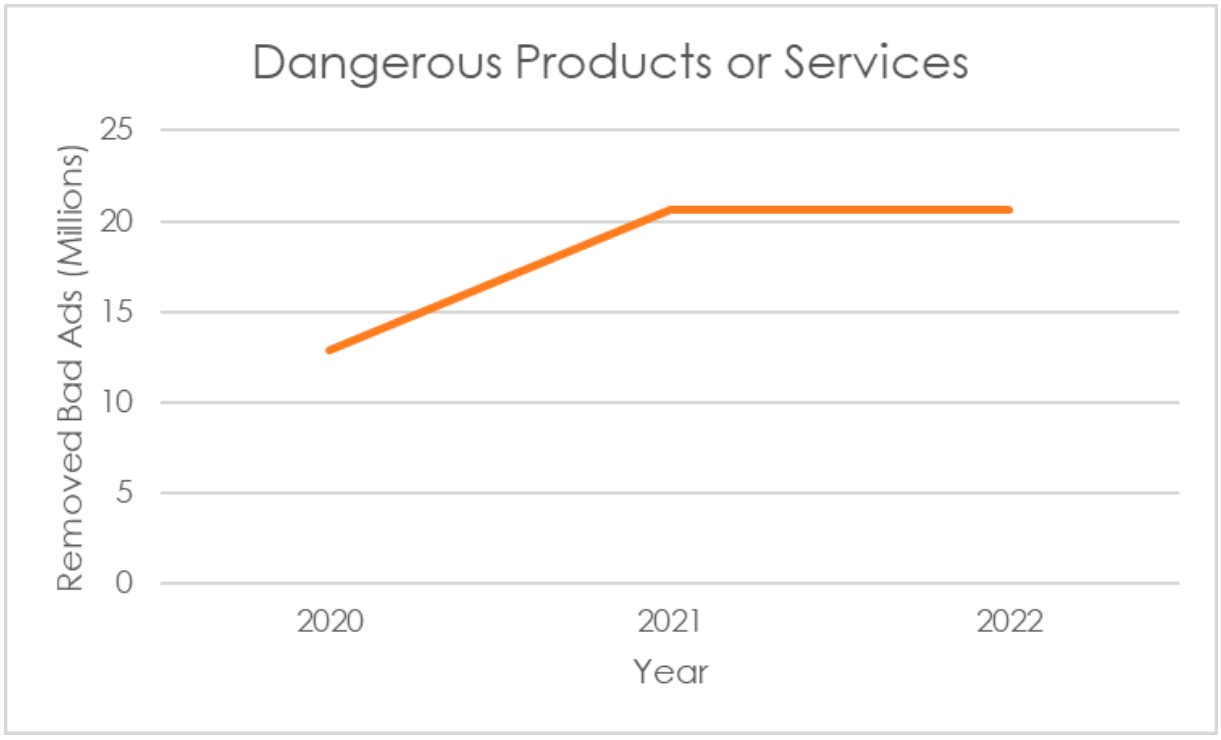


Figure N - Subcategory of Bad Ads Blocked or Removed by Google

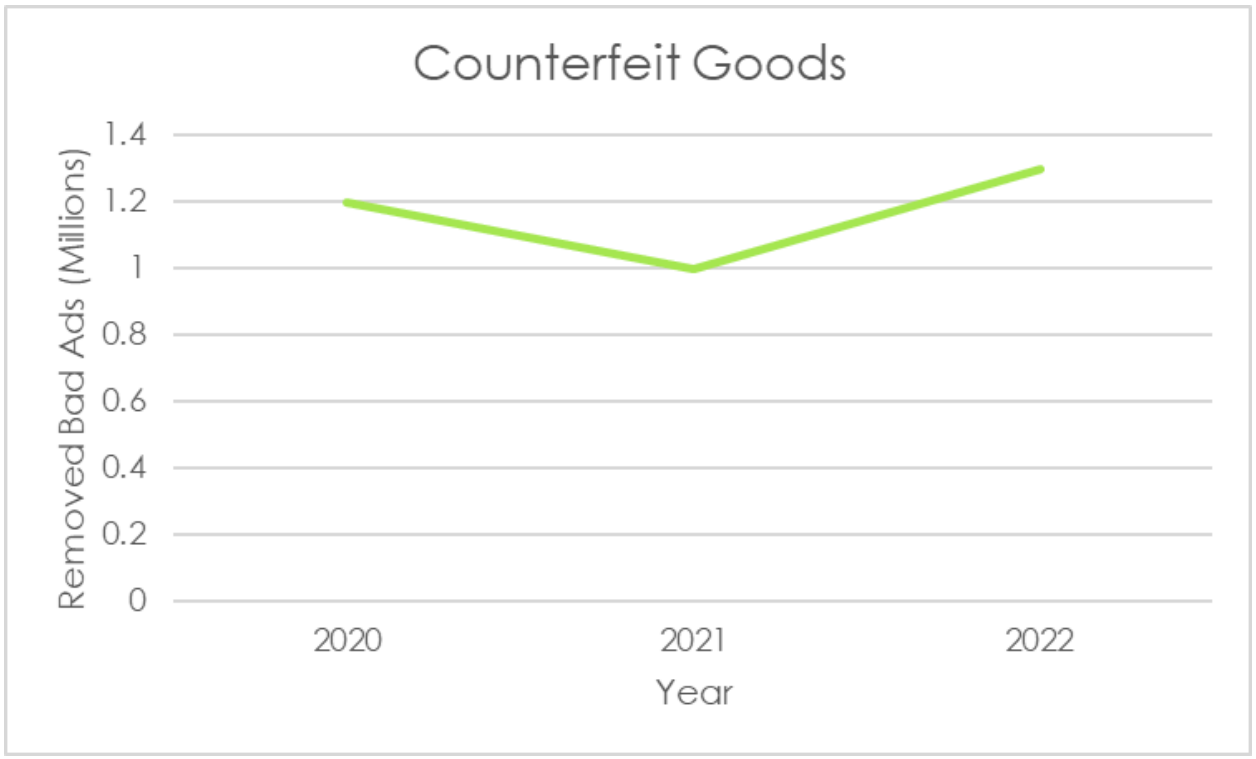


Figure O - Subcategory of Bad Ads Blocked or Removed by Google

Similarly, Google's 2020, 2021, and 2022, Ad Safety Reports list categories of web pages removed year after year. The following graphs demonstrate that Google consistently removed a high volume of web pages for Shocking Content, Sexually Explicit Content, Sexual Content, and Malicious or Unwanted Software. Note that Google began reporting data under the category of Malicious or Unwanted Software in 2021.

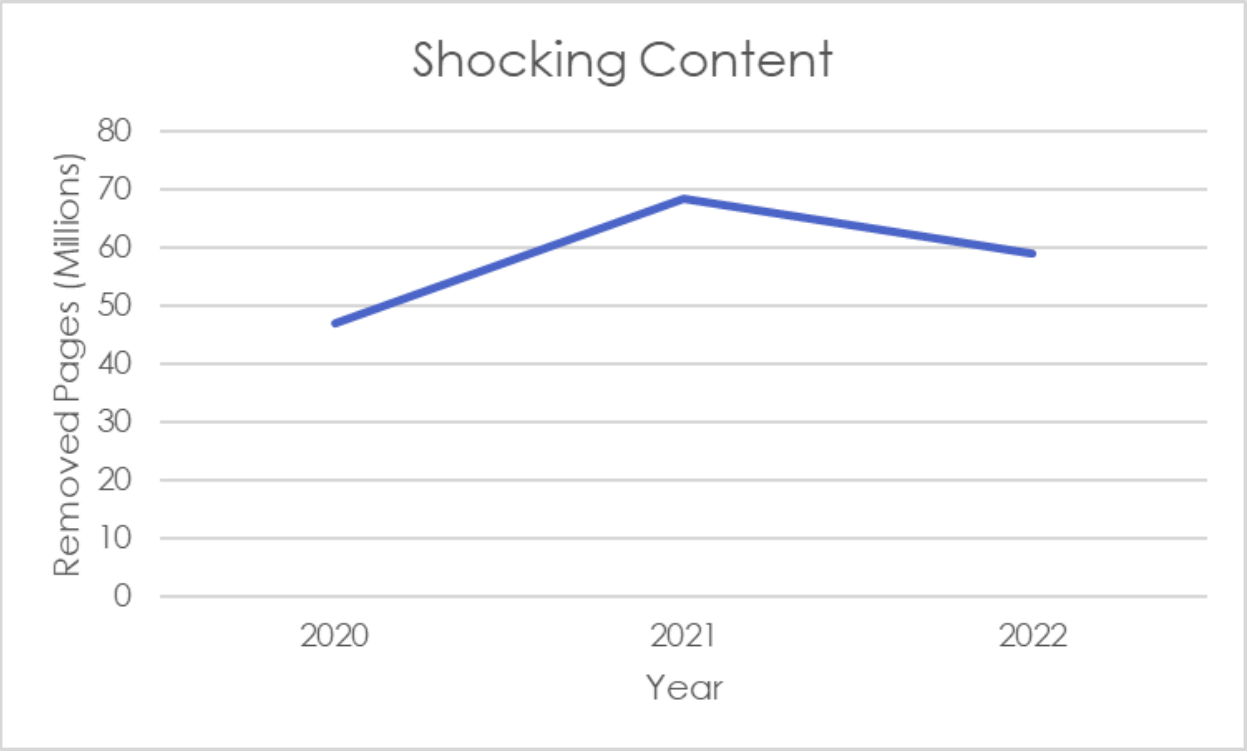


Figure P - Subcategory of Bad Ads Blocked or Removed by Google

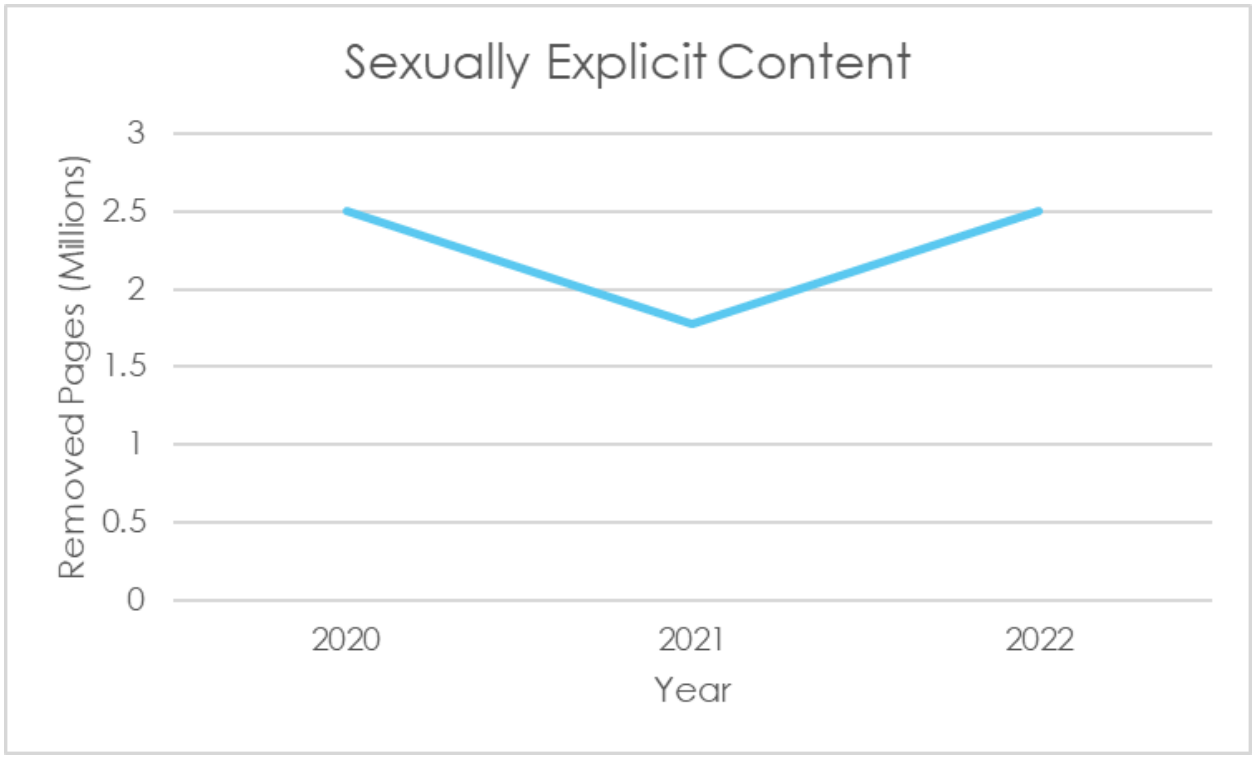


Figure Q - Subcategory of Bad Ads Blocked or Removed by Google

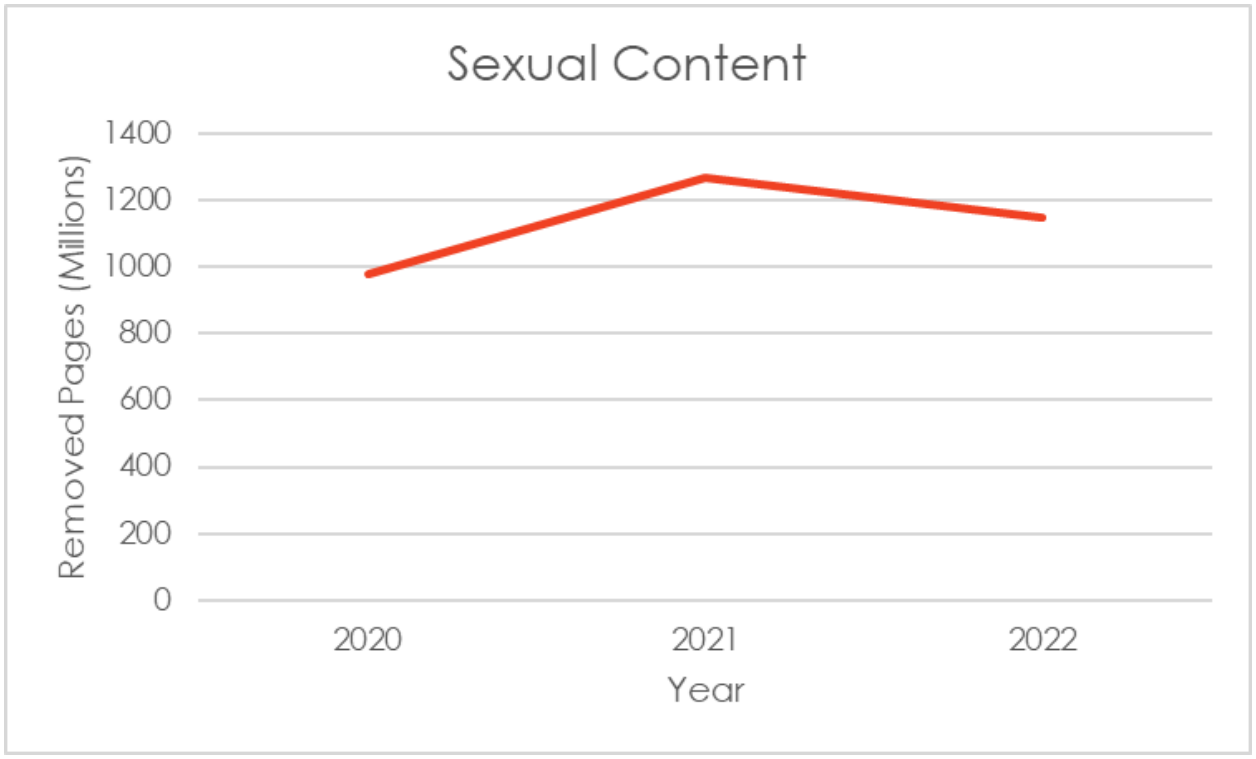


Figure R - Subcategory of Bad Ads Blocked or Removed by Google

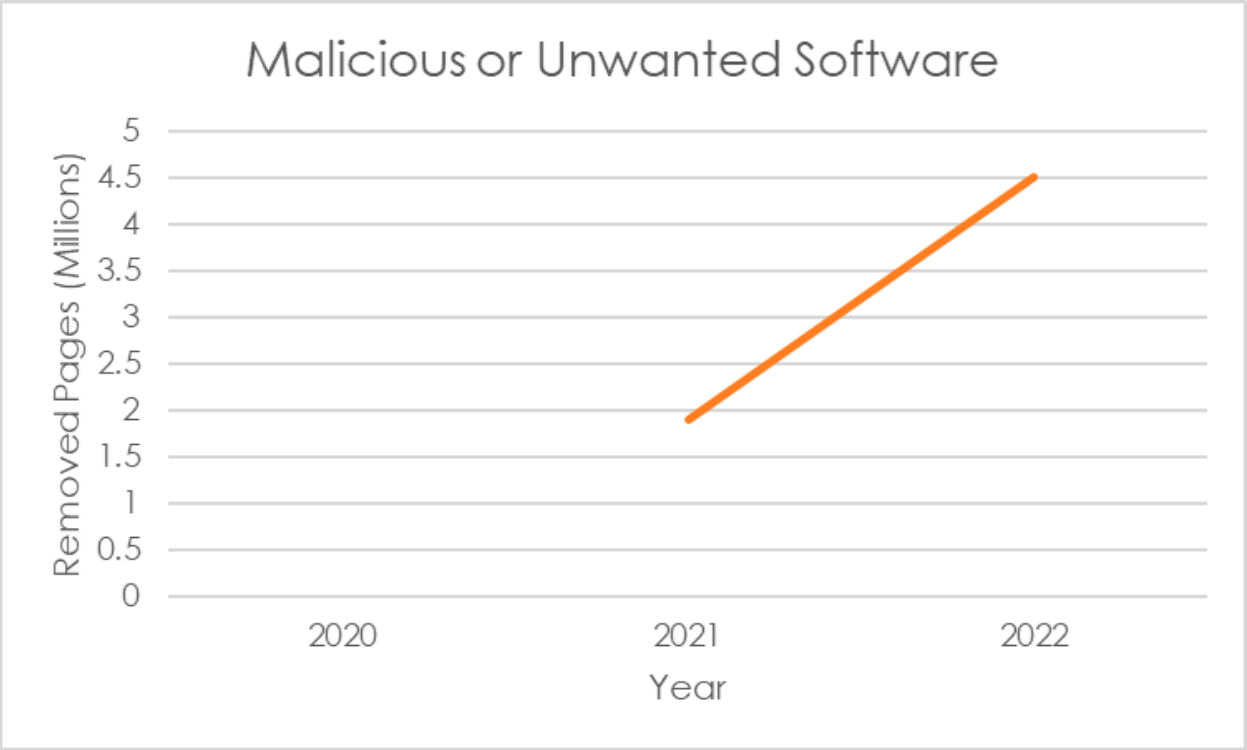


Figure S - Subcategory of Bad Ads Blocked or Removed by Google